CODE ONE

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

BACHELORARBEIT

Herr
Adrian Beutner

Handover im WLAN bei IP-basierter Live-Videoübertragung

2013

Fakultät: Medien

BACHELORARBEIT

Handover im WLAN bei IP-basierter Live-Videoübertragung

Autor:
Herr Adrian Beutner

Studiengang:
Medientechnik

Seminargruppe:
MT09wH-B

Erstprüfer:
Prof. Dipl. Ing. Hans-Joachim Götz

Zweitprüfer:
Dipl. Ing. Boris Kantzow

Einreichung:
Düsseldorf, 28.01.2013

Faculty of Media

BACHELOR THESIS

Wi-Fi seamless roaming for IP-based live-video-broadcasting

author:
Mr. Adrian Beutner

course of studies:
Medientechnik

seminar group:
MT09wH-B

first examiner:
Prof. Dipl. Ing. Hans-Joachim Götz

second examiner:
Dipl. Ing. Boris Kantzow

submission:
Düsseldorf, 28.01.2013

Bibliografische Angaben

Beutner, Adrian

Handover im WLAN bei IP-basierter Live-Videoübertragung

Wi-Fi seamless roaming for IP-based live-video-broadcasting

63 Seiten, Hochschule Mittweida, University of Applied Sciences,
Fakultät Medien, Bachelorarbeit, 2013

Abstract

In dieser Arbeit wird das Handoververhalten einer Videostreamingeinheit im WLAN untersucht. Diese Untersuchung soll klären, ob sich mit WLAN größere Netze mit mehreren Zugangspunkten realisieren lassen, über die IP-basiertes Videostreaming mit CodeOne Hardware und Software betrieben werden kann. Dafür wird WLAN als erstes mit anderen gängigen Marktlösungen für die Kontribution von Videoinhalten verglichen. Im Theorieteil werden dann die Netzwerkgrundlagen sowie die Infrastruktur und Sicherheitsmechanismen von WLAN erklärt. Hierbei wird herausgearbeitet, dass die Authentifizierung der Teilnehmer im WLAN sehr zeitaufwändig und daher im Zusammenhang mit unterbrechungsfreiem Handover problematisch ist. Zudem werden die Grundlagen von Mesh-Netzwerken erläutert. Im Hauptteil werden drei WLAN Systeme untersucht und im Zusammenhang mit der verwendeten Videostreaming-Software der Firma CodeOne verglichen. Grundlegende Vergleichskriterien sind hierbei Betriebssicherheit und Latenzzeit.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AES: Advanced Encryption Standard

AKM: Authentication and Key Management

AP: Access Point

BGAN: Broadband Global Area Network (Satelliten-basierter Kommunikationsdienst)

BPK: Backpack Kit (Mobiler Streaming-Rucksack von CodeOne)

CCMP: Counter-Mode/CBC-MAC Protocol

COFDM: Coded Orthogonal Frequency Division Multiplexing

DFS: Dynamic Frequency Selection

DHCP: Dynamic Host Configuration Protocol

DS: Distribution System

DSL: Digital Subscriber Line

DVB-S: Digital Video Broadcasting – Satellite

DVB-T: Digital Video Broadcasting – Terrestrial

EAP: Extensible Authentication Protocol

GTK: Group Transient Key

HD: High Definition

HTTP: Hypertext Transfer Protocol

IAPP: Inter Access Point Protocol

IEEE: Institute of Electrical and Electronics Engineers

IP: Internet Protocol

ISM: Industrial, Scientific, Medical

IV: Initial Vector

LAN: Local Area Network

LTE: Long Term Evolution (Mobilfunkstandard der 4. Generation)

MAC: Media Access Control

MAP: Mesh-Accesspoint

MP: Mesh-Point

MPEG: Motion Picture Expert Group

MPP: Mesh-Portal

OGM: Originator Message

PDU: Protocol Data Unit

PMK: Pairwise Master Key

PSK: Pre-Shared Key

PTK: Pairwise Transient Key

QPSK: Quadrature Phase Shift Keying

RADIUS: Remote Authentication Dial-In User Service

RSN: Robust Security Network

RTP: Real-Time Transport Protocol

RTMP: Real-Time Messaging Protocol

RTSP: Real-Time Streaming Protocol

SD: Standard Definition

SNG: Satellite News Gathering (Häufig: Fahrzeug für die Satelliten-gestützte TV-Übertragung)

SSH: Secure Shell

SSID: Service Set ID

TCP: Transmission Control Protocol

TKIP: Temporary Key Integrity Protocol

TPC: Transmit Power Control

TTL: Time to live

UDP: User Datagram Protocol

UMTS: Universal Mobile Telecommunications System (Mobilfunkstandard der 3. Generation)

VLAN: Virtual Local Area Network

VPN: Virtual Private Network

WEP: Wired Equivalent Privacy

WLAN: Wireless Local Area Network

WPA: Wi-Fi Protected Access

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

Diese Bachelorarbeit ist im Zeitraum Juli 2012 bis Januar 2013 bei der CodeOne GmbH entstanden. Sie soll an die Diplomarbeit von Dipl. Ing Christian Leykam anknüpfen, der die grundsätzliche Eignung von Wireless LAN für IP-basierte Live-Videoübertragung bereits untersucht und validiert hat.

Ich möchte mich ganz herzlich beim gesamten CodeOne-Team für die Unterstützung bedanken, insbesondere bei Boris Kantzow, Sven Hanten und Christian Leykam für die Hilfe bei der Themenfindung und die Betreuung meiner Arbeit, sowie Christian Michels für die tatkräftige Unterstützung bei den Tests. Zudem gilt mein Dank der Firma Airberry und Steffen Dreise für die zur Verfügung gestellte Teststellung ihrer Mesh-Systemlösung.

Als letztes gilt mein Dank Prof. Hans-Joachim Götz, der die Betreuung meiner Bachelorarbeit von der Hochschulseite aus übernommen hat und mein Interesse an der Programmverbreitung schon im Jahr 2011 geweckt hat.

1 Einleitung

1.1 Motivation: Rundfunk in konvergenten Netzen

Klassische IT-Strukturen und -Netze sind heutzutage eng vermascht mit der Rundfunktechnik. Bis vor wenigen Jahren waren diese Strukturen und Netze noch nicht weit entwickelt genug, um den hohen Anforderungen durch die Rundfunktechnik gerecht zu werden. Mittlerweile sind sie jedoch, gerade was Speicherplatz und Bandbreiten betrifft, soweit entwickelt, dass die aktuellen Entwicklungen in der Rundfunktechnik nicht mehr ohne Informationstechnologie auskommen. Konvergente Netzwerke halten Einzug in Studios, Funk- und Produktionshäuser, lösen verschiedenste proprietäre Netzwerktechnologien ab und machen zum Beispiel bandlose Workflows möglich.[1]

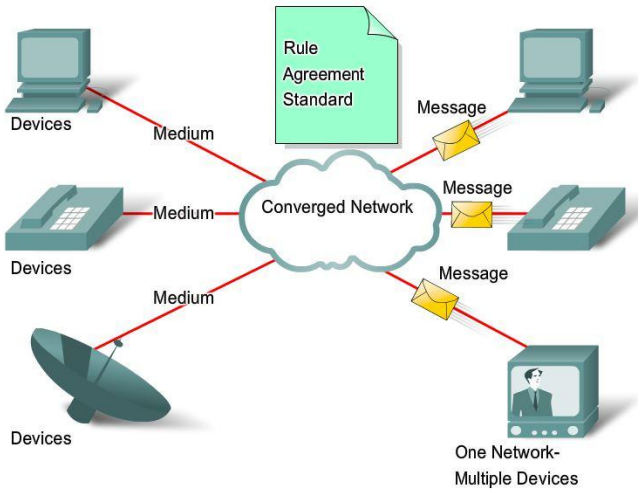


Abbildung 1: Konvergentes Netzwerk[2]

Wesentlicher Bestandteil dieser Workflows ist der paketbasierte Dateiaustausch. Dieser paketbasierte Dateiaustausch ist Kerneigenschaft von konvergenten Netzen und basiert auf dem Internet Protocol (IP). IP-basierte Workflows sind für Medienunternehmen aus vielen Gründen reizvoll: Beispielsweise sind die Verbindungen bidirektional und es können mehrere Dienste gleichzeitig über eine Verbindung übertragen werden. Zudem ist Verteilung der Daten im gesamten Netzwerk und auch die Weiterverteilung ins Internet sehr einfach.

[1] Vgl. Blaeß, Seite 13ff
[2] Cisco

Zitat des Marktführers für Netzwerktechnik Cisco Systems:

Traditional telephone, radio, television, and computer data networks each have their own individual versions of the four basic network elements (Fault Tolerance, Scalability, Quality of Service and Security). In the past, every one of these services required a different technology to carry its particular communication signal. Additionally, each service had its own set of rules and standards to ensure successful communication of its signal across a specific medium.

Technology advances are enabling us to consolidate these disparate networks onto one platform - a platform defined as a converged network. The flow of voice, video, and data traveling over the same network eliminates the need to create and maintain separate networks. On a converged network there are still many points of contact and many specialized devices - for example, personal computers, phones, TVs, personal assistants, and retail point-of-sale registers - but only one common network infrastructure.[3]

1.2 IP-basierte Live-Videoübertragung

IP-basierte Live-Videoübertragung ist eine verhältnismäßig neue Technologie, die auf konvergenten Netzwerken basiert. Mit dieser Technologie beschäftigt sich die Firma CodeOne aus Düsseldorf. Sie betreibt damit Kontribution: Für den Transport des Videostreams von der Kamera ins Haus greift CodeOne vornehmlich auf Mobilfunknetze der dritten und vierten Generation (UMTS und LTE) zurück. Diese Netze basieren ebenfalls auf IP. Mobilfunknetze haben den Vorteil, dass Live-Videoübertragung, im Gegensatz zu klassischen Systemlösungen, wie SNG, ortsunabhängig[4] möglich ist. Außerdem ist zumindest UMTS mittlerweile fast flächendeckend verfügbar, der Rollout von LTE findet zurzeit statt. Der entscheidende Nachteil bei Mobilfunknetzen ist jedoch, dass sie öffentlich nutzbar und bei starker Auslastung nicht mehr betriebssicher sind. Zudem gestaltet sich auch der Handover, also der Wechsel von einer Mobilfunkzelle in die nächste, sehr schwierig. Solide Bandbreiten können nicht gewährleistet werden.[5] Um diesem Problem zu begegnen, hat die Firma CodeOne damit begonnen, WLAN-Netze als Übermittlungsmedium zu erforschen. Idee ist der Aufbau eines privaten Infrastrukturnetzwerkes mit mehreren Zugangspunkten, zwischen denen sich die Kamera

[3] Cisco
[4] Vgl. Bönninghoff, Seite 1
[5] Vgl. Leykam, Seite 1

frei bewegen kann. Die Weiterleitung ins Internet erfolgt von einem vorher definierten, zentralen Punkt, beispielsweise einer Regie. Hier kann entweder eine feste Leitung zum Einsatz kommen oder eine Satellitenverbindung oder eben auch Mobilfunknetze wie UMTS oder LTE.

1.3 Bisheriger Forschungsstand und Problemstellung

Ergebnis der Untersuchungen von CodeOne ist, dass sich WLAN, aufgrund der hohen Bandbreiten, sehr gut für Live-Videoübertragung eignet. Allerdings ist der Wechsel von einem Zugangspunkt zum nächsten noch nicht möglich: Dieser Wechsel kann nur in gewissem Maße zentral gesteuert werden, vielmehr entscheidet jedes Endgerät selber wie schnell es wechseln möchte.[6] Bisher bricht das Videostreaming beim Verlassen der Funkzelle ab. Dadurch ist die Reichweite einer auf WLAN basierenden Lösung auf einen Accesspoint beschränkt.

1.4 Zielstellung

Ziel dieser Bachelorarbeit ist es daher, das Handoververhalten einer Videostreaming-Einheit im WLAN gezielt zu untersuchen und zu optimieren, damit mit WLAN größere Netze mit mehreren Zugangspunkten aufgebaut werden können. Außerdem sollen „echte“ Mesh-Komponenten, also ein System aus mehreren Zugangspunkten, die drahtlos miteinander kommunizieren, untersucht werden. Denn es wird vermutet, dass sich der Wechsel von einem Mesh-Zugangspunkt zum nächsten deutlich einfacher gestaltet als bei klassischen WLAN-Systemen.

[6] Vgl. Leykam, Seite 107

2 Bestehende Systemlösungen: „Smarte Produktionsmittel“

In einem großen Medienunternehmen, nehmen wir mal an einer öffentlich-rechtlichen Rundfunkanstalt wie dem Westdeutschen Rundfunk, kommen für die Live-Videoübertragung inzwischen verschiedenste mobile Produktionsmittel zum Einsatz. Kriterien für die Auswahl des Produktionsmittels sind in erster Linie die Größe und die Spontanität der Produktion, sowie natürlich die journalistischen Inhalte, die übertragen werden sollen. Die bestehenden Systemlösungen lassen sich grob einteilen in satellitengestützte Produktionsmittel (SNG) und Funk: Hierbei gilt: Klassische Drahtloskamera-Technik wird nur dafür verwendet, um ein Signal die ersten Meter von der Kamera zu einer Regie zu übertragen. SNG’s liefern dagegen fertige Fernsehsignale an den Schaltraum des Senders. Daneben gibt es aber auch in den großen Produktionshäusern einen Trend zu kleineren neuen Produktionsmitteln, wie die Streaming-Rucksacklösungen von CodeOne, Spiegelreflexkameras wie die Canon EOS 5D oder Actionkameras wie die Go Pro Hero. Gerade dieses „kleinere Besteck“ ermöglicht nämlich ganz neue Formate und Ergänzungen zum laufenden Programm im Internet.[7] Zudem sind diese Produkte deutlich günstiger als klassische Fernsehtechnik und benötigt weniger Personal. Gemeinsame Eigenschaft vieler neuer Produktionsmittel ist die einfache Bedienung. Diese muss mittlerweile nicht mehr nur durch extra dafür geschulte Spezialisten, wie zum Beispiel SNG-Operator erfolgen, sondern zum Beispiel auch durch Kameramänner oder Cutter. Moderne Produktionsmittel arbeiten computergestützt, beispielsweise bei der Suche nach Satelliten. Der WDR bezeichnet daher seine neuen mobilen Produktionsmittel als „smart“.[8]

2.1 Satellitengestützte Produktionsmittel

Satellitengestützte Produktionsmittel bauen für den Signaltransport eine Sichtverbindung zu einem Satelliten auf (Uplink). Dieser Satellit verstärkt das Signal und schickt es zurück zur Erde (Downlink). Das Signal kann überall in der Ausleuchtzone des Satelliten (Footprint) empfangen werden. Die Satelliten befinden sich im sogenannten geostationären Orbit in ca. 36000 km Höhe. Während des Transports muss das Signal diese Strecke zweimal zurücklegen. Es bewegt sich mit Lichtgeschwindigkeit und benötigt für diese Strecke rund 0,25 Sekunden: 72000 Km / 300000 Km/s = 0,24s

[7] Vgl. WDR Print
[8] Vgl. WDR Flyer

2.1.1 „Klassische Produktionsmittel“

Klassische, satellitengestützte Produktionsmittel sind in der Regel in Anschaffung und Betrieb die teuersten Produktionsmittel, bieten jedoch hohe Qualität und Einsatzsicherheit. Sie arbeiten nach dem DVB-S Standard. Zur Übertragung wird das Signal als MPEG-Transportstrom enkodiert, anschließend auf ein Trägersignal aufmoduliert. Je nach gewünschter Qualität (SD oder HD) und Bandbreite kommen verschiedene Kompressions- und Modulationsverfahren zum Einsatz, zum Beispiel MPEG 2 mit QPSK und einer Datenrate von 8,44 MBit/s.[9] Je nach Anwendungsfall wird in der „Bauform“ der Produktionsmittel unterschieden. Es gibt SNG-Vans, Sprint-Cams und Flyaways. SNG-Vans sind besonders gut für mittelgroße Produktionen geeignet.

Abbildung 2: Großer SNG-Van des WDR mit ND Satcom Satellitentechnik

Es handelt sich dabei um Fahrzeuge, die auf großen Lieferwagen basieren. SNG-Vans besitzen Bildmischer und Schnittplätze, somit können bei der Live-Schalte mehrere Kameras zum Einsatz kommen, zudem können vorher produzierte Beiträge eingespielt werden. Sprint-Cams sind abgerüstete SNG’s, sie dienen lediglich dazu, das Signal einer Kamera live abzusetzen. Zudem können sie als Uplink-Fahrzeug bei großen Produktionen dienen. Flyaways sind stationäre Uplinks. Ihr Vorteil liegt darin, dass sie sich sehr einfach auf- und abbauen lassen. Zudem sind sie besonders leicht. Flyaway’s sind dafür ausgelegt, mit dem Flugzeug transportiert zu werden.

[9] Vgl. Leykam, Seite 4

2.1.2 „Neue Produktionsmittel“

Auch bei der Satellitenübertragung hat ein Umdenken stattgefunden: Seit ca. 2 Jahren werden Internetanbindungen über Satellit angeboten, welche breitbandähnliche Datenraten anbieten. Diese bidirektionalen Satellitenverbindungen werden von den beiden europäischen Satellitenbetreibern SES Astra und Eutelsat angeboten und nutzen das Ka-Band.

Abbildung 3: Toowaysat: Satellitenschüssel und Modem für Internetverbindung

Die Datenraten, die mit IP-SAT-Verbindungen erreicht werden können, reichen aus, um damit Videostreaming zu realisieren: Bei Toowaysat lassen sich beispielsweise Flatrates mit Datenraten bis zu 6 MBit/s Upstream und 18 MBit/s Downstream buchen.[10] Im Unterschied zu festen DSL-Leitungen oder LTE-Verbindungen kommt es allerdings aufgrund der großen Entfernungen zum Satelliten zu Verzögerungen bei der Datenübertragung. Das hat Auswirkungen auf interaktive Anwendungen wie Online-Games, Remote-Desktops oder Videotelefonie:[11] Hier sind die Verbindungen bidirektional: Der Client schickt eine Anfrage zum Server, der Server generiert eine Antwort und schickt diese zurück an den Client. Für einen Frage-Antwort Prozess müssen Daten also zweimal ins All und wieder zurück, müssen also insgesamt 144000 km zurücklegen, bevor sich auf dem Computer des Nutzers irgendetwas tut. Entsprechend gibt es Latenzen von einer halben Sekunde oder mehr. Bei unidirektionalen Anwendungen wie Filetransfer oder Streaming hat das Delay, das durch die große Entfernung ent-

[10] Vgl. Tooway

[11] Breitbandbüro, Seite 6

steht, allerdings kaum Auswirkungen. Für Online-Games ist eine Internet-Satellitenverbindung also nicht zu empfehlen, für Broadcaster ist sie dagegen sehr interessant, weil sich, im Gegensatz zum klassischen SNG, verhältnismäßig günstig hohe Datenraten übermitteln lassen.

2.1.3 Inmarsat BGAN

Abbildung 4: BGAN Explorer 727 von Thrane & Thrane

Das mobile, satellitengestützte Produktionsmittel BGAN nimmt bei der Berichterstattung eine Sonderrolle ein. Denn im Gegensatz zu anderen Produktionsmitteln ist die Übertragungsqualität sehr stark begrenzt: IP-basiertes Videostreaming ist mit einer garantierten Datenrate von 384 KBit/s möglich.[12] Inmarsat BGAN ist ein eigenes Satellitennetz und dient dazu weltweit Telefonie, Standard-IP- und Streaming-IP-Übertragung zu ermöglichen: Drei Satelliten decken die gesamte Erdoberfläche bis auf die Polkappen ab. Das macht das Handling sehr einfach: Während beim klassischen SNG genau geplant werden muss, welcher Satellitenbetreiber welche Länder abdeckt, kann man mit BGAN-Terminals „einfach loslegen“: Die Bezahlung kann mit Prepaidtarifen erfolgen. Zudem sind BGAN-Terminals sehr kompakt und extrem schnell auszurichten. Bei Bedarf kann sogar eine Tracking-Antenne zum Einsatz kommen, somit kann die die Dateiübertragung, ähnlich wie bei GPS, auch aus fahrenden Fahrzeugen erfolgen. Für Broadcaster ist BGAN trotz der schlechten Übertragungsqualität ein beliebtes Produktionsmittel, gerade bei der Berichterstattung aus Krisengebieten.

[12] Inmarsat, Seite 6

2.2 Funklösungen für drahtlose Kameras

Der Bedarf nach drahtlosen Kameras ist immer dann besonders groß, wenn keine Kabel verlegt werden dürfen oder hohe Mobilität gefordert ist. Analoge Technik konnte diesen Bedarf nur bedingt decken. Seit ca. zehn Jahren werden für drahtlose Videoproduktionen jedoch digitale Funkstrecken eingesetzt, die einerseits spektakuläre Bilder zum Beispiel aus Rennwagen oder Helikoptern liefern können, andererseits hohe Betriebssicherheit auch da bieten, wo keine Kabel verlegt werden dürfen. Außerdem ist es möglich, größere Areale über Gleichwellennetze abzudecken. So wird zum Beispiel die SNG-freie Berichterstattung aus dem Regierungsviertel in Berlin möglich.[13]

Abbildung 5: Link L1500 Wireless HD/SD Transmitter

Digitale Funkstecken basieren auf DVB-T oder auf proprietären Abwandlungen dieses Standards. Die Übertragung der Signale erfolgt über Coded Orthogonal Frequency Division Multiplexing (COFDM): Das digitale Kamerasignal wird komprimiert und mit Fehlerschutz versehen, anschließend wird es in einem Mehrträgerverfahren[14] übertragen. Durch den Einsatz eines Guard-Intervalls[15] kann der bei terrestrischer-Übertragung übliche Mehrwege-Empfang[16] zur Verstärkung des Signals genutzt werden.[17] Die Eignung einer auf DVB-T basierten Funkstrecke für die Hochschule Mittweida wurde 2008 untersucht. Als Ergebnis wurde festgehalten, dass für den

[13] Meixelsberger, Seite 8

[14] Mehrträgerverfahren: Die Informationen werden nicht einer einzigen Trägerfrequenz übertragen, sondern auf viele Unterträger aufgeteilt

[15] Guardintervall: Zeitraum, in dem alle eintreffenden Signale zu einem Summensignal zusammengefasst werden

[16] Mehrwegeempfang: Durch Reflexion an Gebäuden und anderen Hindernissen kann ein Nutzsignal mehrfach mit unterschiedlichen Laufzeiten am Empfänger eintreffen

[17] Meixelsberger, Seite 25

störungsfreien Betrieb der untersuchten Funklösung Shark Sender C.106 und Empfänger C.100 auf jeden Fall eine Sichtverbindung zwischen Sender und Empfänger notwendig ist.[18] Erfahrungen des CodeOne Teams mit Riedel-Funkstrecken zeigen jedoch, dass gute Ergebnisse auch ohne Sichtverbindung erreicht werden können.

2.3 Mobilfunklösungen

Seit ca. 2 Jahren drängen Systemlösungen auf den Markt, welche die Encodierung eines Kamerasignals als IP-Stream und die Weiterverteilung über Mobilfunknetze ins Internet in einem kompakten Gerät zusammenfassen. Ähnlich wie bei Sprint-Cams kann man mit diesen Rucksacklösungen fertige Fernsehbilder liefern: Sobald die Daten nämlich im Internet sind, können sie entweder an einer Gegenstelle wie einem Schaltraum abgegriffen werden und dort weiterverarbeitet werden (Unicast) oder direkt zum Zuschauer gebracht werden (Webcast). Abstriche müssen allerdings bei der Bildqualität gemacht werden: Zwar arbeitet das verwendete H264 sehr effektiv, SNG-ähnliche Qualität kann jedoch nur bei optimalen Bedingungen, zum Beispiel durch die Nutzung von LTE erreicht werden.

Abbildung 6: CodeOne Backpack Kit v2 ohne Rucksack

[18] Meixelsberger, Seite 72

Die Distribution über Mobilfunknetze setzt eine Bündelung mehrerer Mobilfunkkanäle und eine variable Lastverteilung (Load Balancing) voraus, weil Mobilfunknetze öffentlich nutzbar sind und bisher keine „Quality of Service“ bieten können. Ein Produkt, das diese Voraussetzungen erfüllt ist der Multichannel VPN Router der Firma Viprinet. Das CodeOne Backpack Kit v1 ist eine Kombination aus Software-Encoder und einem abgewandelten Viprinet-Router. Ein Nachfolger des Backpackkits mit eigener Bündelungstechnik ist zurzeit in Arbeit.

2.4 Bedarfsanalyse WLAN

IP-basiertes Videostreaming im WLAN verknüpft die Eigenschaften einer drahtlosen Kamera mit der einer konvergenten Netzstruktur: Mit WLAN-Zugangspunkten, die drahtlos untereinander kommunizieren, können einfach große Netze aufgebaut werden, in denen man sich mit einer Kamera - ein unterbrechungsfreier und zuverlässiger Handover vorausgesetzt - frei bewegen kann. Neben dem sicheren Handover ist außerdem eine möglichst kurze Signalverzögerung nötig. Klassische Funklösungen haben mittlerweile Verzögerungszeiten von 1-2 Frames, also kleiner 100ms. Diese Werte werden mit einer WLAN-Lösung erst mal nicht erreichbar sein, hier sollten 1000ms angepeilt werden. Solange genügend Bandbreite zur Verfügung steht, ist es zudem möglich, dass mehrere Kameras das gleiche Netz nutzen, eine Arbeitsweise, die mit herkömmlichen drahtlosen Kamerasystemen nicht möglich ist. Auch die Übertragung von zusätzlichen Diensten wie N-1, Kommando oder sogar Steuerdaten ist denkbar.

Videosignale, die über WLAN transportiert werden, können sehr einfach weiterverbreitet werden: Im Prinzip ist nur ein Routing ins Internet notwendig. Für die Weiterleitung der Daten ins Internet könnte eine günstige IP-SAT-Verbindung zum Einsatz kommen. Eine aufwändige und teure Signalwandlung wie bei der Kombination aus DVB-T-Funkstrecke und klassischem SNG entfällt dagegen. Großer Unterschied zu Mobilfunknetzen ist, dass es sich bei WLAN um ein privates Netz handelt. Wünschenswert wäre, dass WLAN dort nutzbar ist, wo öffentliche Netze wie UMTS völlig überlastet sind, beispielsweise bei einem Großevent wie einer Kirmes oder einem Festival.

3 Theorieteil – Netzwerk-Grundlagen

3.1 ISO/ OSI Referenzmodell:

Telekommunikation dient dazu, eine Ende-zu-Ende Übertragung von Inhalten zu ermöglichen,[19] wie die Abfrage von Mails von einem Mailserver, ein Telefonat oder die Übertragung von Fernsehbildern vom CodeOne Rucksack ins Web. An dieser Telekommunikation sind viele Komponenten beteiligt, von denen die Nutzer im Idealfall nur sehr wenig mitbekommen. Seit 1984 gibt es ein Kommunikationsmodell, das sämtliche beteiligten Komponenten klar strukturiert. Es wird Referenzmodell für die offene Kommunikation OSI (Open System Interconnection) genannt und wurde von der International Standardization Organisation (ISO) erarbeitet. Das ISO/ OSI-Referenzmodell teilt den Kommunikationsprozess in sieben Schichten ein, wobei der Nutzer mit der höchsten (siebten) Schicht agiert. Letzten Endes funktioniert jede Telekommunikation über Strom, Wellen oder Licht. Diese sog. Medien bilden die erste, physische Schicht des Modells. Allen anderen Schichten obliegt es, das Agieren des Nutzers in Signale (Bits) umzuwandeln, die über Strom, Wellen oder Licht übertragen werden können. Außerdem soll eine sichere und möglichst fehlerfreie Übertragung gewährleistet werden. Dabei ist es egal, ob der Nutzer gerade im Internet surft, Videos dreht oder telefoniert.

Ebene Layer	Bezeichnung Deutsch/Englisch	Beschreibung	Funktion
Schicht 1	Physik Physical	Übertragungsmedium, mechanische und elektrische Eigenschaften der Schnittstellen	Bittransport über Kupfer- oder Glasfaserkabel bzw. Funk
Schicht 2	Sicherung Data Link	Übertragungsprotokoll mit Korrekturmechanismus für Übertragungsfehler	Datenrahmen; Erkennung von Bitfehlern und ggf. Korrektur
Schicht 3	Netzwerk Network	Netzwerkprotokoll für die Bereitstellung von Verbindungen (Vermittlung = Switching)	Adressierung Routing und Paketfragmentierung
Schicht 4	Transport Transport	Das Ende-zu-Ende-Transport-Protokoll sorgt für die Vollständigkeit der Informationen	Bildung von PDUs aus den Anwendungsdaten
Schicht 5	Kommunikationssteuerung Session Control	Das Sitzungsprotokoll steuert den Verbindungsaufbau und verwaltet den gesamten Kommunikationsvorgang	Wiederaufsatzpunkt Benutzeridentifikation Kostenzuordnung

[19] Winkler: Grundlagen KT3, Seite 2

Schicht 6	Darstellung Presentation	Das Präsentationsprotokoll definiert die Darstellung der Information auf dem Ausgabeterminal	Benutzeroberfläche Verschlüsselung
Schicht 7	Anwendung	Spezifische Protokolle für Anwendungen	Textverarbeitung Datenbankabfrage

Tabelle 1: OSI-Referenzmodell[20]

Ein Allgemeines Beispiel für die Funktionsweise des OSI-Modells gibt folgender Satz:

„ A Web Browser application renders an HTML presentation, which is delivered using an http session, over a TCP transport connection, via an IP network, over an Ethernet data link, using twisted-pair physical Cabel"[21]

Für Videostreaming mit WLAN könnte der Satz wie folgt lauten:

„Eine Decoder-Anwendung greift einen MPEG-Container ab. Dessen Start wurde über eine RTSP-Sitzung befohlen. Die Daten werden über RTP sortiert und über UDP transportiert, über ein IP-basiertes Netzwerk, welches aus WLAN- und Ethernet-Komponenten besteht und als Übertragungsmedium sowohl elektromagnetische Wellen als auch Kupferleitungen nutzt."

3.2 Internet Protocol

Das Internet Protocol (IP) ist tatsächlich Basis des heutigen „World Wide Webs" Jeder Teilnehmer, (man spricht hier von Host) eines IP-basierten Netzwerks, üblicherweise ein Computer oder ein Router bekommt eine IP-Adresse zugewiesen. Diese Adresse ist 32 Bit lang (IPv4). Die IP-Adresse setzt sich zusammen aus Netzadresse und Hostadresse. Die Unterteilung erfolgt durch die Netzmaske:

- Netzmaske: 255.255.255.0
- IP-Adresse: 192.168.10.11

[20] Kafka, Seite 62
[21] Perkins, Seite 18

Hierbei ist die Zahl 11 die Hostadresse im Netzwerk 192.168.10.0. Verschiedene Hosts im selben Netzwerk (z.B. 192.168.10.11 und 192.168.10.22) können direkt miteinander kommunizieren. Wenn ein Host in einem anderen Netzwerk erreicht werden soll (z.B. 192.168.20.33), müssen die Nutzdaten geroutet werden. Für diese Kommunikation zwischen den Netzwerken sind Router zuständig:

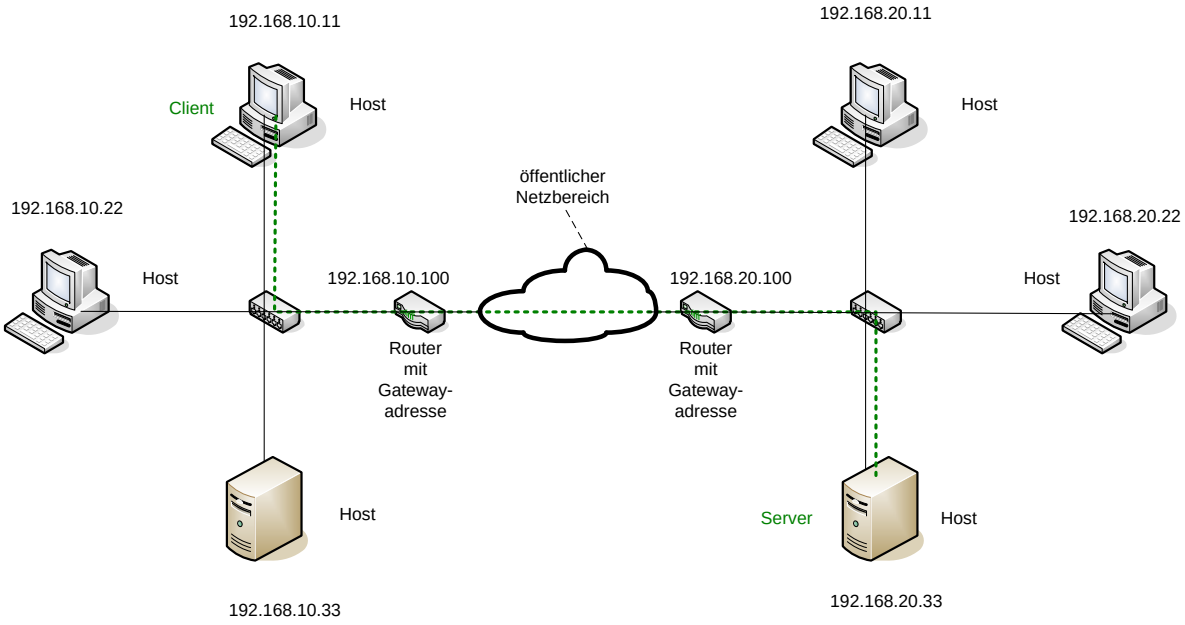


Abbildung 7: Routing zwischen zwei Netzwerken

Jeder Router ist über eine Gateway-Adresse in ein Netzwerk eingebunden. Soll ein Host außerhalb dieses Netzwerks erreicht werden, wird ein Datenpacket an den Router geschickt. Anhand von Routing-Tabellen ermittelt der Router die beste Route und schickt das Paket an den nächsten Router weiter.

Da der Adressraum von IPv4, also rund 4,3 Milliarden IP-Adressen, so gut wie aufgebraucht ist, findet zurzeit das Rollout des Nachfolgers IPv6 statt. Bei IPv6 wurde der Adressraum auf 2^128 Bits vergrößert, die IP-Adressen werden nun in hexadezimaler Schreibweise angegeben. An der grundsätzlichen Idee, Hosts und Router mit logischen Adressen zu versorgen, um Daten paketorientiert über ein Netzwerk zu verschicken, wird sich aber auch in Zukunft nichts ändern.

3.3 Transportprotokolle

Aufgabe von Transportprotokollen ist es, in einem Netzwerk eine Ende-zu-Ende Kommunikation zwischen Anwendungen zu ermöglichen. Hierzu werden IP-Pakete (mit

Empfänger- und Absenderadresse) um einen Quell- bzw. Zielport ergänzt und zu Segmenten zusammengefasst. Der Vorteil von Segmenten gegenüber konstanten Datenströmen ist, dass mehrere Dienste gleichzeitig als Multiplex übertragen werden können. Die wichtigsten Transportprotokolle sind UDP und TCP.

3.3.1 User Datagram Protocol

Das User Datagram Protocol ist ein verbindungsloses Transportprotokoll. Eigentlich beinhaltet es nur minimale Erweiterungen zu IP, wie Quell- und Zielport, sowie einem Length-Feld und einer Checksumme. Eine Kontrolle der Daten findet nicht statt und Packetverluste werden hingenommen. Entsprechend obliegt es bei einer Kommunikation über UDP den Schichten fünf bis sieben die eingegangenen Daten zu kontrollieren, zu ordnen und ggf. neu anzufordern. UDP arbeitet in Echtzeit und ist daher für zeitkritische Anwendungen wie VoIP oder auch Videostreaming sehr interessant.

3.3.2 Transmission Control Protocol

Das Transmission Control Protocol ist ein verbindungsorientiertes Transportprotokoll. Bei einer Kommunikation über TCP können eigentlich keine Daten verloren gehen. Im Gegensatz zu UDP nämlich werden die verschickten Segmente vom Empfänger quittiert (Acknowledge). Bleibt eine Quittierung aus gilt das Segment als verloren und wird erneut versendet. Zudem erhalten die Pakete eine Sequenznummer. Am Empfänger werden die Daten gepuffert, um anhand der Sequenznummern richtig sortiert werden zu können. Dadurch können jedoch nicht so hohe Datenraten erzielt werden wie bei UDP. Die Datenrate einer TCP-Verbindung wird im Wesentlichen bestimmt durch die Fenstergröße: Jedes Segment muss in einem bestimmten Zeitfenster übertragen werden. Bei fehlerfreier Übertragung eines Segments wird die Fenstergröße langsam additiv erhöht. So können mehrere Segmente in einem Zeitfenster übertragen und zusammen durch eine Quittung bestätigt werden. Die Datenrate einer TCP Verbindung steigt solange langsam an bis Paketverluste gemeldet werden. Das veranlasst den Netzwerktreiber der Quelladresse die Datenrate rapide zu reduzieren, um sie dann wieder langsam zu erhöhen.

3.4 Streamingprotokolle

Aufgabe von Streamingprotokollen ist es, eine Echtzeitübertragung von Video- und Audiodaten über IP-basierte Netze zu ermöglichen. Es gibt zahlreiche Anwendungsbereiche, wie IP-Telefonie, Webcast und Videokonferenzsysteme. Streamingprotokolle sind im OSI-Modell über den Transportprotokollen angesiedelt.

3.4.1 Real-Time Transport Protocol

Ein weit verbreitetes Protokoll ist das Real-Time Transport Protocol, das auf UDP basiert. RTP ergänzt die UDP-Datagramme um Sequenznummern, Zeitmarken und eindeutige Identifikationsnummern. So können die Daten verbindungsorientiert verschickt werden. Anhand der Sequenznummern erkennt RTP ob Verluste aufgetreten sind, außerdem können anhand der Zeitmarken Audio- und Videodaten synchronisiert werden. Zudem enthält RTP Informationen über den Payload-Type, also zum Beispiel den verwendeten Codec für Audio und Video.

3.4.2 Real-Time Streaming Protocol

Das Real-Time Streaming-Protocol dient zur Steuerung von Streaming-Sessions und ähnelt damit in seiner Funktion HTTP: Bei HTTP können Webinhalte mit den Befehlen GET und POST angefordert oder abgeschickt werden: Bei RTSP können Medienströme über Befehle wie Play, Pause, Record oder Teardown kontrolliert werden. Diese Befehle können zudem in Web-Player integriert werden. Damit wird RTSP quasi zur Internet-Fernsteuerung. Allerdings ist RTSP nicht kompatibel zu Adobe Flash. Die Adressierung einer RTSP Sitzung erfolgt über eine URL, ähnlich HTTP, zum Beispiel:

- rtsp://server_ip:port/app_name/stream_name
- rtsp://192.168.10.88:1935/live/handover

3.4.3 Real-Time Messaging Protocol

Das Real-Time Messaging Protocol ist ein proprietäres Protokoll von Adobe Systems, dass auf TCP basiert und damit größere Latenzen aufweist als RTP. Es wurde 2009 von Adobe offengelegt. RTMP dient als Protokoll für die Übertragung von Daten zwischen Adobe Flash Plattformen, typischerweise einem Flash-Encoder, einem Flash Streaming-Server und einem Flash-Player. Die beiden Komponenten Flash Encoder und Flash Player sind kostenlos erhältlich, der Flashplayer ist zudem als Plug-In auf den meisten Web-Browsern installiert. Dadurch bietet sich RTMP besonders für Webcast-Anwendungen an. Flash Streaming-Server sind für die Vervielfältigung der RTMP-Streams zuständig. So können mit Flash mehrere tausend User gleichzeitig erreicht werden.

4 Theorieteil – WLAN

4.1 Grundlagen

Wireless Local Area Network ist ein Standard, der dazu dient, Computer drahtlos miteinander zu vernetzen. WLAN wurde 1997 als Standard 802.11 von dem IEEE verabschiedet.[22] In den vergangenen 15 Jahren wurde der WLAN-Standard ständig der Zeit bzw. der Rechenleistung von Computern angepasst: Die gängigsten Neuerungen waren die Anpassung der Datenrate und die Standardisierung von Sicherheitsmechanismen. Dadurch nimmt die Verbreitung von WLAN ständig zu, mittlerweile ist WLAN fester Bestandteil des Lebens und der Arbeit, egal ob zuhause, im Büro oder unterwegs. Typische Anwendungen sind der kabellose Internetzugang oder die schnurlose VoIP-Telefonie im Unternehmen. In den letzten drei Jahren hat sich WLAN so rasant entwickelt, dass es inzwischen hoch spezialisierte Anwendungen gibt, wie die kabellose Vernetzung von Sensoren in der Industrie. Daher ist es naheliegend, WLAN auch für IP-basiertes Videostreaming in Betracht zu ziehen. Hier werden aber besonders hohe Anforderungen an das WLAN gestellt: Das sind hohe Bandbreiten für die Übertragung von hochauflösendem Fernsehen in Kombination mit kurzer Latenz für Live-Übertragung und unterbrechungsfreiem bzw. sicherem Handover für hohe Mobilität. In dieser Kombination liegt die ganze Problematik: Bisher gibt es nämlich wenig Anwendungen, welche auf diese Kombination angewiesen sind: Beispielsweise werden für den Internetzugang zuhause für die Übertragung von Multimediainhalten hohe Anforderungen an die Bandbreite gestellt, auf Mobilität und Latenz wird hier jedoch kaum Wert gelegt. Andersherum ist man bei VoIP-Telefonie auf kurze Latenz, unterbrechungsfreien Handover und gleichzeitig sichere Verbindungen angewiesen, für Audiosignale reichen jedoch wenige Kilobytes an Übertragungsrate aus.

4.2 Überblick über die wichtigsten Standards

Die Erweiterungen innerhalb des 802.11 WLAN-Standards werden mit einem Kleinbuchstaben deklariert.

[22] Vgl. Lüders, Seite 157

Jahr	Bezeichnung	Bemerkung	Beschreibung
1997	802.11	Basisstandard	Übertragungsraten von bis zu 2 MBit/s auf 2.4 GHz
1999	802.11a	Erweiterung: Keine Kompatibilität zu b	Übertragungsraten von bis zu 54 MBit/s auf 5 GHz
1999	802.11b	Erweiterung: Keine Kompatibilität zu a	Übertragungsraten von bis zu 11 MBit/s auf 2.4 GHz
2003	802.11f	Erweiterung	IAPP für standardisierte Kommunikation im DS
2003	802.11g	Erweiterung von b	Übertragungsraten von bis zu 54 MBit/s auf 2.4 GHz
2003	802.11h	Erweiterung von a	Einführung von TPC und DFS für die optimale Nutzung des 5 GHz Bandes
2004	802.11i	Erweiterung von a,b,g	Überarbeitung der Sicherheitsfeatures
2005	802.11e	Erweiterung von g,a,	QoS für zeitkritische Anwendungen (VoIP)
2008	802.11r	Erweiterung	Standard für Fast Roaming bei zeitkritischen Anwendungen (VoIP)
2008	802.11s	Erweiterung	Standardisiertes Routingprotokoll für Mesh
2009	802.11n	Erweiterung von g,a	Übertragungsraten von bis zu 600 MBit/s auf 2.4 GHz und 5 GHz

Tabelle 2: Zeitstrahl Entwicklungen von WLAN, Bruttodatenraten[23]

4.3 Technische Spezifikationen

Mit „Wireless Local Area Network“ ist schon sehr viel über die Eigenschaften dieses Netzes gesagt: Denn WLAN genauso wie LAN dient im Wesentlichen dazu, IP-Packete zu verschicken. Der Data Link Layer wurde größtenteils vom LAN-Standard übernom-

[23] Vgl. Rech, Seite 409

men und um Managementoperationen ergänzt.[24] Wichtige Managementoperationen sind die Quittierung von Frames[25] und die Authentifizierung der Teilnehmer. Auf Authentifizierung wird in Kapitel 4.4 genauer eingegangen. Größter Unterschied zu LAN ist das Übertragungsmedium: Statt Kupferleitungen werden hier elektromagnetische Wellen benutzt. Jede elektromagnetische Welle hat eine bestimmte Frequenz. Bei Überlagerung von zwei gleichen Wellen kommt es zu Störungen.

4.3.1 Rechtliche Aspekte

Daher werden Frequenzen in Deutschland streng von der Bundesnetzagentur überwacht. Für die Nutzung von WLAN stehen in Deutschland das 2.4 GHz Band (ISM) mit den Kanälen 1-13 sowie das 5 GHz Band mit den Kanälen 36,40,44,48,52,56,60,64 und 100,104,108,112,116,120,124,128,132,136,140 zur Verfügung. Auch die Sendeleistungen sind fest vorgeschrieben: So darf WLAN auf 2.4 GHz mit maximal 100 mW betrieben werden, bei 5 GHz sind 200mW erlaubt. Zudem darf im Outdoorbereich auf den hohen Kanälen ab Kanal 100 mit 1 W gesendet werden[26], allerdings nur mit Aktivierung von TPC und DFS.[27]

4.3.2 WLAN Infrastruktur:

Adhoc (Independant BSS)

Möchte man zwei Geräte über WLAN direkt miteinander vernetzen, sollte der Adhoc-Modus gewählt werden. Der Adhoc-Modus ist quasi Kabelersatz. Geräte, die über Adhoc miteinander verbunden sind, sind vollkommen gleichberechtigt. Notwendig für den Adhoc-Betrieb sind die Einstellung derselben SSID und Verschlüsselung, sowie desselben Kanals an allen Geräten. Zudem müssen die IP-Adressen festgelegt werden. Die Adhoc-Konfiguration ist für die direkte Verbindung von zwei oder mehr Laptops nicht sehr attraktiv, da hier sämtliche Parameter für WLAN manuell konfiguriert werden müssen. Eine deutlich größere Rolle kommt dem Adhoc-Modus beim Mesh (Kapitel 4.8) zu.

---

[24] Vgl. Sauter, Seite 337
[25] Vgl. Sauter, Seite 356
[26] Bundesnetzagentur: WLAN
[27] Rech, Seite 18

Infrastructure BSS

Die Bereitstellung eines drahtlosen Internetzugangs funktioniert nicht allein über Funk. Hierfür ist WLAN-Infrastruktur notwendig. Zum Aufbau einer solchen WLAN Infrastruktur gehören ein Accesspoint (AP) und mindestens ein Client, zum Beispiel ein Laptop. Der AP fungiert dabei als Schnittstelle zum drahtgebundenen Netzwerk: Will also ein Client zum Beispiel eine Breitband-DSL-Leitung nutzen, verbindet er sich über Funk mit dem AP. Dieser leitet den IP-Traffic vom Client über Kabel in das Distribution System (eine Art Ethernet-gebundener Backbone) weiter. Von dort aus kann dann der IP-Traffic ins Internet geroutet werden. Ein Netzwerk, das aus mehreren Clients und genau einem AP besteht wird Basic Service Set (BSS) genannt.

4.3.3 Einschub: SSID und Frequenzen

Damit der AP von den Clients erkannt wird strahlt er wie ein Leuchtturm in bestimmten Abständen die Service Set ID (SSID) aus. Da die SSID von allen Clients im Sendebereich des APs erkannt werden soll, strahlt er diese als Broadcast (Point to Multipoint) ab. Der normale Verkehr funktioniert dagegen über Unicast (Point to Point). Die Kommunikation im WLAN funktioniert nicht allein über eine Welle mit einer Frequenz. Vielmehr wird ein Frequenzbereich mit einer bestimmten Bandbreite und einer Mittenfrequenz benutzt. Bei WLAN spricht man hierbei von Kanälen. Mit dem Begriff „Frequenz“ ist also stets die Mittenfrequenz gemeint. Die Bandbreite eines Kanals ist 25 MHz, allerdings stehen im ISM-Band 13 Kanäle mit einer Bandbreite von nur 5 MHz zur Verfügung. Für einen reibungslosen WLAN-Betrieb dürften also nur die Kanäle 1,6 und 11 genutzt werden. Das ist in der Praxis jedoch kaum machbar, da das 2.4 GHz Band sehr stark ausgelastet ist. Auf dem 5 GHz Band ist die Situation dagegen deutlich entspannter, da sich keine Kanäle überlappen.

Abbildung 8: Screenshot InSSIDer: WLAN Auslastung 2.4 GHz bei CodeOne am 19.10.2012

Abbildung 8 zeigt die WLAN Auslastung auf dem 2.4 GHz Band am CodeOne Arbeitsplatz: Es konnten sieben verschiedene SSIDs ermittelt werden, welche sich gegenseitig teilweise sehr stark überlappen.

ESS und Handover

Um die Reichweite eines WLANs zu vergrößern, können mehrere BSS zusammengeschaltet werden. Hierzu werden die APs über das Distribution System (DS) miteinander verbunden. Bei einem WLAN mit mehreren APs spricht man von einem Extended Service Set (ESS). Wichtig bei einem ESS ist, dass alle APs dieselbe SSID ausstrahlen. Damit es nicht zu Störungen kommt, müssen die APs auf unterschiedlichen Frequenzen senden. Damit ein ESS reibungslos funktioniert, ist es unbedingt empfehlenswert, die Kanäle 1,6 und 11 zu verwenden. Für einen Client, der zwischen den APs wechseln möchte, bedeutet das, dass er seine Empfangsfrequenz vom alten AP auf den neuen AP umstellen muss. Das ist der erste, sozusagen physikalische Teil des Handovers.

4.4 Sicherheit allgemein

Die Unterscheidung zwischen BSS und ESS geht meistens einher mit der Unterscheidung zwischen den beiden Anwendungsbereichen Home und Business. Bei Home-Anwendungen wird WLAN meistens dazu gebraucht, um eine kabellose Internetverbindung bereitzustellen. Der AP ist daher meistens Bauteil eines IP-Routers, der die Datenpakete ins Internet weiterleitet. Der Bedarf nach mehreren Funkzellen ist praktisch nicht vorhanden. Bei Home-Anwendungen gibt es vor allem den Bedarf nach hohen Datenraten, beispielsweise für Videostreaming. Die Sicherheitsanforderungen sind dagegen geringer.

In einem Unternehmen dagegen wird WLAN meist von mehreren APs bereitgestellt um die Gesamtreichweite des drahtlosen Netzwerkes zu erhöhen. Unternehmen sind im Gegensatz zu Home-Anwendern essentiell auf hohe Sicherheit angewiesen. Diese Sicherheitsmechanismen machen vor allem die Anmeldung des Clients am AP sehr langwierig. Gerade für VoIP-Telefonie wird jedoch ein schneller Übergang von einem AP zum nächsten AP gefordert. Das ist der zweite sozusagen Management-Teil des Handovers. Um schnellen Handover zu ermöglichen, werden also Managementoperationen gebraucht, die einerseits hohe Sicherheitsanforderungen erfüllen, diese aber in kürzester Zeit abarbeiten. Daher sollen im Folgenden die gängigen Sicherheitsfeatures dargelegt und anschließend verschiedene Möglichkeiten für schnellen Handover diskutiert werden.

4.4.1 Unverschlüsselt

Ein offenes, unverschlüsseltes Netzwerk kann jedes WLAN-fähige Endgerät nutzen. Das ist für sogenannte Hotspots interessant: An Bahnhöfen, Flughäfen o.Ä. sind diese offenen Netze oft vertreten, hier wird davon ausgegangen, dass die Nutzer dieser Netze ständig wechseln. Allerdings muss dem Nutzer klar sein, dass sämtlicher Datenverkehr zwischen Endgerät und AP mitgeschnitten werden kann. Hier liegt es in der Verantwortung des Nutzers, sich durch speziellen Maßnahmen wie zum Beispiel einem VPN-Tunnel zu schützen.[28] Für WLANs in Privathaushalten und in Unternehmen kommen diese unverschlüsselten Netzwerke nicht in Frage. Während Privatanwender vor allem daran interessiert sind, dass ihr Netzwerk nicht von fremden Personen genutzt wird und ihnen Ärger mit dem Provider erspart bleibt, sind Unternehmen vor allem daran interessiert, dass ihre sensiblen Daten nicht mitgeschnitten werden können.[29] Entsprechend die Sicherheitsanforderungen um ein Vielfaches höher als bei Privatanwendern, was sich auch in den Sicherheitsstandards niederschlägt.

4.4.2 WEP

Eine überholte, aber dennoch oft anzutreffende Art der Verschlüsselung ist Wired Equivalent Privacy (WEP). WEP ist Teil des 802.11g, b und a Standards und verwendet für die Verschlüsselung einen Stream Ciphering-Algorithmus. Die Originaldaten werden mithilfe einer Cipherfrequenz verschlüsselt, welche aus einem Initial Vector (IV) und einem Key berechnet wird. Während sich der IV für jedes Frame ändert, wird der Key manuell festgelegt und gilt für alle Nutzer des Netzwerkes.[30] Zudem wird der IV, wie alle anderen Management- und Steuersignale bei WEP unverschlüsselt übertragen, nur die Nutzdaten und die Checksumme werden verschlüsselt.[31] Es gibt inzwischen zahlreiche Programme, die mit Hilfe des im Klartext übertragenen IV den Schlüssel nach etwa 5-6 Millionen übertragenen Datenpaketen berechnen können.[32]

[28] Sauter, Seite 383
[29] Vgl. Rech, Seite 429ff
[30] Sauter, Seite 384
[31] Winkler, Folie 68
[32] Sauter, Seite 384

4.4.3 802.11i

Um die Schwachstellen von WEP zu beheben, wurde von der IEEE der 802.11i Standard entwickelt und im Juni 2004 verabschiedet. 802.11i sieht sowohl Maßnahmen für die Verschlüsselung als auch für die Authentifizierung vor. Dabei sollte die Kompatibilität zu älteren WLAN-Geräten gewahrt werden. Aus diesem Grund wurde das optionale Verschlüsselungsverfahren Temporary Key Integrity Protocol (TKIP) eingeführt, dass sich über Treiber- bzw. Firmware-Aktualisierung auf älteren Geräten implementieren lässt. Das endgültige Verschlüsselungsverfahren basiert auf dem Advanced Encryption Standard (AES).

Das erweiterte Authentifizierungsverfahren, das in 802.11i Anwendung findet, wird als Authentication and Key Management (AKM) bezeichnet. AKM basiert entweder auf Pre-Shared Key (PSK) oder auf dem 802.1X Standard mit EAP. Während PSK gut bei kleinen WLANs funktioniert, sollte 802.1X nur für größere Netzwerke verwendet werden, da es einen Authentifizierungsserver voraussetzt.[33]

Die Sicherheitsdefizite bei WEP veranlassten die Netzwerkindustrie, sprich die Wi-Fi Alliance, bereits im Jahr 2003 einen eigenen Standard zu definieren. Dieser Standard wird Wi-Fi Protected Access (WPA) genannt und basiert auf dem Stand der 802.11i Erweiterung von 2003 mit TKIP als Verschlüsselungsverfahren. Unterschieden wird in WPA Personal und WPA Enterprise, bei WPA Personal geschieht die Authentifizierung mit PSK, bei WPA Enterprise mit 802.1X.

Im September 2004 wurde mit WPA2 dem aktuellen 802.11i Rechnung getragen: Für die Verschlüsselung wurde AES vorgeschrieben. Damit entspricht WPA2 in allen Sicherheitsmechanismen 802.11i. Abstriche wurden allerdings bei der Unterstützung von schnellem Roaming gemacht: Auch diese müssen laut 802.11i Standard unterstützt werden, wurden aber bei WPA2 nicht übernommen.[34] Stattdessen greifen die Hersteller auf proprietäre Maßnahmen zurück, so wird schnelles Roaming oft nur dann möglich, wenn AP und Client im ESS vom selben Hersteller stammen.[35]

Lösungsansätze für schnellen Handover setzen ein schnelles AKM voraus. Daher lohnt es sich, sich mit den Methoden PSK und 802.1X bzw. EAP genauer zu beschäftigen.

---

[33] Vgl. Rech, Seite 449ff
[34] Vgl. Rech, Seite 451ff
[35] Vgl. Rech, Seite 50

4.5 Authentifizierung und Schlüsselmanagement (AKM)

4.5.1 Pre-Shared Key

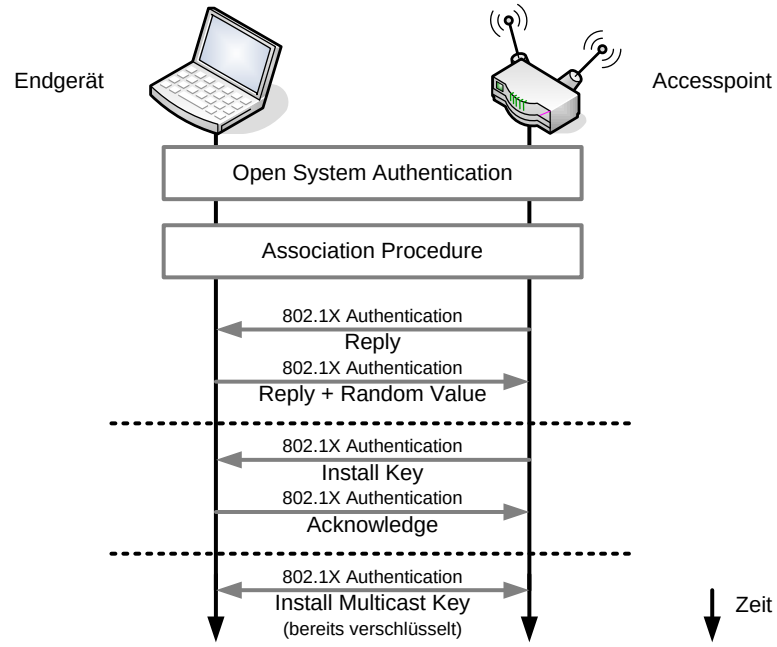


Abbildung 9: WPA-PSK-Authentifizierung und Schlüsselaustausch[36]

Beim PSK-Verfahren wird unabhängig von der eigentlichen Authentifizierung im Endgerät und im AP die gleiche Passphrase (Pre-Shared Key) hinterlegt, mit deren Hilfe die eigentlichen Schlüssel generiert werden: Für den Verbindungsaufbau sendet der AP eine Zufallszahl an das Endgerät. Daraufhin generiert das Endgerät aus der Zufallszahl und dem Pre-Shared Key eine Antwort und schickt diese mit einer weiteren Zufallszahl zurück an den AP. Der AP vergleicht die Antwort mit der zuvor selber aus dem Pre-Shared Key berechneten Antwort. Wenn bei Endgerät und AP die gleiche Passphrase verwendet wird, stimmen beide Antworten überein. Nach erfolgreicher Prüfung ist das Endgerät authentifiziert, der AP sendet ihm nun den Pairwise Master Key (PMK) zu, welcher wieder mit dem PSK verschlüsselt wird. Nach der Entschlüsselung quittiert das Endgerät den Erhalt des PMKs. Daraufhin beginnt die Verschlüsselung der Daten in beide Richtungen. Als letztes teilt der AP dem Endgerät den

[36] Sauter, Seite 386 (bearbeitet)

Schlüssel für die Broadcast-Frames mit GTK. Diese Nachricht ist bereits verschlüsselt.[37][38]

4.5.2 802.1X

802.1X ist ein Authentifizierungsstandard, der als „Port based Network Access Control“ bezeichnet wird und ursprünglich für drahtgebundene Netze entwickelt wurde. Schwächen im Hinblick auf WLAN wurden jedoch im Jahr 2004 behoben. Das 802.1X Verfahren stützt sich auf drei Instanzen, dem Supplicant (Client), dem Authenticator (AP) und dem Authentifizierungsserver. Die sog. Ports sind logische Zugangspunkte ins Netzwerk. In 802.1X wird zwischen unkontrollierten und kontrollierten Ports unterschieden. Die Idee dahinter ist, dass die Authentifizierung des Clients und eventuell die Nutzung grundlegender Dienste wie DHCP[39] über den unkontrollierten Port erfolgen. Erst nach erfolgreicher Authentifizierung, das heißt nach der Übermittlung des Schlüssels durch den Authentifizierungsserver, erlaubt der Authenticator dem Client auf den kontrollierten Port zuzugreifen.[40] Damit hat der Client vollen Zugriff auf das Netzwerk.

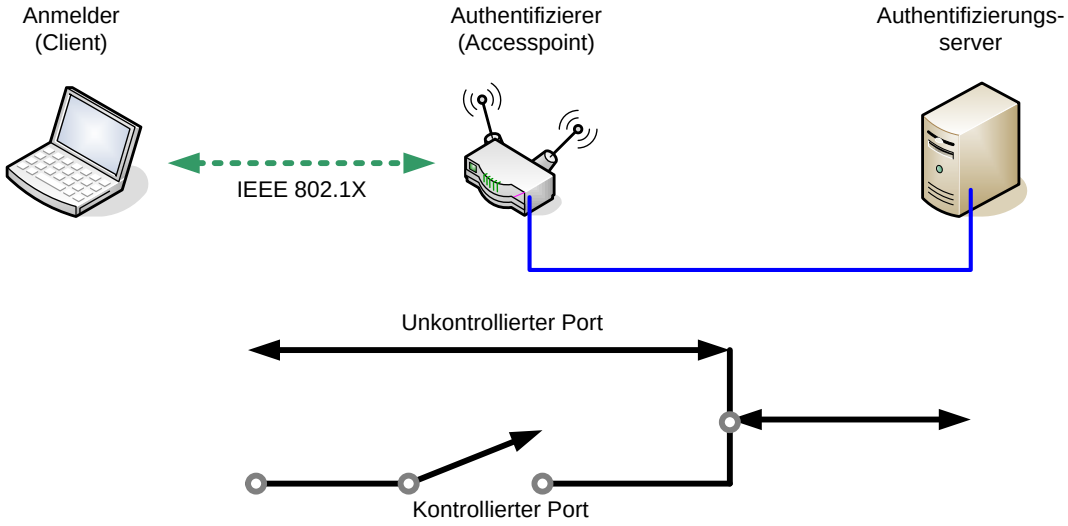


Abbildung 10: Die Verwendung von 802.1X in 802.11i[41]

[37] Vgl. Sauter, Seite 387
[38] Vgl. Rech, Seite 474
[39] Vgl. Rech, Seite 456
[40] Vgl. Kafka, Seite 219
[41] Kafka, Seite 220 (bearbeitet)

Als Authentifizierungsserver kommen RADIUS-Server zum Einsatz, sind entweder im WLAN Controller integriert oder Teil der LAN-Netzwerkstruktur. RADIUS-Server übernehmen in Netzwerken die Aufgaben Authentifizierung, Autorisierung und Abrechnung. Der Authenticator dient als Vermittler zwischen Supplicant und Authentifizierungsserver als sog. EAP-Proxy. Als Verständigung dieser drei Instanzen dient EAP.

4.5.3 EAP Überblick:

„Das Extensible Authentication Protocol beschreibt in einem einfachen Request-Response-Verfahren den Austausch von Authentifizieungsdaten vom Benutzer zum Authentifizierungsserver und dessen Antwort.“[42] Der Authentifizierungsvorgang wird vom Client (Supplicant, zu Deutsch Bittsteller) eingeleitet. Dieser greift auf den Port des Authenticators zu und sendet ein EAP-Start-Frame aus. Der Authenticator fordert den Supplicant daraufhin auf, sich zu identifizieren (siehe Abbildung 11).

Abbildung 11 Screenshot HSMW-Eduroam: Anmelde-Aufforderung[43]

Nach dem Empfang der Daten schickt der Authenticator die Daten weiter an den Authentifizierungsserver. Dieser vergleicht die Daten mit einer Datenbank und entscheidet. Daraufhin weist er den Authenticator entweder an, nach einem Fehlschlag der Authentifizierung den kontrollierten Port nicht zu aktivieren. Der Client verbleibt somit auf dem unkontrollierten Port, an der Hochschule Mittweida wird der Nutzer erneut aufgefordert, Benutzername und Passwort einzugeben. Nach erfolgreicher Authentifizierung sendet der Authentifizierungsserver die Meldung „RADIUS/EAP Success“ und an

[42] Rech, Seite 457
[43] HSMWiki: Eduroam Einrichtung unter Windows 7

den Authenticator und das Schlüsselmaterial an den Supplicant. Der Authenticator schaltet daraufhin den kontrollierten Port für den Client frei.[44]

4.6 802.11i-Implementierungen für schnelles Roaming

Wie gezeigt wurde, sind bei Authentifizierung und Schlüsselmanagement bei 802.11i viele Schritte zwischen den drei Instanzen Supplicant, Authenticator und Authentifizierungsserver notwendig, bis der PMK erzeugt wurde. Der 802.1X Authentifizierungsprozess benötigt, bis der PMK erzeugt ist, ca. 700ms[45], was zu erheblichen Störungen bei Echtzeitanwendungen führt. Der Zustand, der zu diesem Zeitpunkt erreicht wurde wird Pairwise Master Key Security Association (PMKSA) genannt. Danach erfolgt die Generierung von PTK und GTK sehr schnell, daher können die dafür notwendigen Handshakes bei zeitkritischer Betrachtung vernachlässigt werden.[46]

PMKSA-Caching

Die Idee hinter PMKSA-Cashing ist, den Zustand PMKSA im AP zu speichern. Dafür muss der Client sich aber notwendigerweise schon einmal beim AP authentifiziert haben, bzw. die komplette 802.11i-Authentifizierung durchlaufen haben. Statt eine komplette 802.1X Authentifizierung abzuarbeiten, authentifizieren sich Client und AP mit dem zwischengespeicherten PMKSA. „Für jede aufgebaute PMKSA zwischen Client und Authentifizierer wird eine eindeutige Identifikation, der Pairwise Master Key Identifier (PMKID), erzeugt“[47]. Diese PMKID wird bei der Assoziierung zwischen Client und AP ausgetauscht. Anhand dessen prüft der AP ob der entsprechende PMKSA zwischengespeichert ist. Wenn das der Fall ist, müssen daraufhin nur noch PTK und GTK neu generiert werden.[48]

Pre-Authentication

Hauptaugenmerk bei dem Pre-Authentication Verfahren ist, dass der Client selber nach anderen AP’s in Reichweite sucht, noch bevor die Verbindung zum aktuellen AP kritisch wird bzw. abbricht. Dazu muss der Client einen Scan durchführen, was entspre-

[44] Vgl. Rech, Seite 457
[45] Stüntz, Seite 6
[46] Rech, Seite 475
[47] Stüntz, Seite 6
[48] Vgl. Rech, Seite 476

chend Bandbreite benötigt. Hat der Client einen neuen bevorzugten AP gefunden, führt er eine Authentifizierung mit dem neuen AP durch, noch während er mit dem alten AP verbunden ist. Dazu teilt er dem alten AP den Wechsel mit. Dieser leitet dann sämtliche Daten, die zur 802.1X Authentifizierung notwendig sind über das DS an den neuen AP weiter. Zudem leitet er auch noch eventuell zwischengespeicherte Daten an den neuen AP weiter. Sobald die Authentifizierung abgeschlossen ist, kann der Client direkt einen 4-Wege-Handshake mit dem neuen AP durchführen.[49]

Die drahtgebundene Kommunikation zwischen den APs war lange nicht standardisiert. Stattdessen hat die Netzwerkindustrie auf proprietäre Protokolle zurückgegriffen, um die Kommunikation zu ermöglichen. Erst im Jahr 2003 wurde der 802.11f Standard veröffentlicht, welcher das Inter Access Point Protocol (IAPP) für die Kommunikation von verschiedenen APs im selben DS vorsieht.[50]

4.7 Zusammenfassung 802.11i

Größtes Problem bei der Bewertung der Roaming-Mechanismen von 802.11i ist die Tatsache, dass 802.11i von den wenigsten Endgeräten vollständig unterstützt wird. WLAN Adapter sind häufig nur auf WPA2 Personal ausgelegt. Das heißt, sie unterstützen zwar PSK, aber nicht die Roaming-Mechanismen von 802.11i. Das bedeutet, dass jeder Client selbstständig entscheidet, wann er wechseln möchte. Die Regeln, an die er sich dabei zu halten hat, werden von jedem WLAN-Chip-Hersteller proprietär festgelegt und greifen je nach Hersteller unterschiedlich gut: Somit kann es sein, dass ein WLAN-Chip von Broadcom oder Intel ein besseres Handoververhalten aufweist als WLAN-Chip von Atheros oder Ralink. Um einen zuverlässigen Handover zu erzielen, muss deshalb die richtige Kombination aus WLAN-Infrastruktur-Komponenten und Clients gefunden werden.

4.8 Von Adhoc zum Mesh

WLAN-Accesspoints und -Router sind im Grunde genommen abgespeckte, kleine Computer. Wie eingangs erwähnt können Computer, die über Funkmodule verfügen, direkt drahtlos über den Adhoc-Modus miteinander verbunden werden. Diese Konfiguration lässt sich nun auch auf Accesspoints übertragen: So kann zwischen mehreren

[49] Vgl. Rech, Seite 476
[50] Vgl. Rech, Seite 50

Accesspoints ein drahtloses DS für die direkte Kommunikation untereinander aufgebaut werden. Dieses drahtlose DS wird Mesh genannt.

Als Sicherheitsmechanismus kann eine CCMP-Verschlüsselung über ein gemeinsames Passwort verwendet werden. Diese Methode wird WPA-NONE genannt. Sicherer ist IBSS/RSN, diese Methode ähnelt PSK: Es werden paarweise Sitzungen aufgebaut, die Station mit der niedrigeren MAC-Adresse übernimmt die Rolle des Supplicant und die Station mit der höheren die Rolle des Authenticators.[51]

In der Theorie[52] bestehen Meshed Networks aus mehreren Knoten, die sich redundant miteinander verbinden. Es gibt drei Komponenten, Mesh-Accesspoints (MAPs), Mesh-Points (MPs) und und Mesh-Portals (MPPs): Mesh-Accesspoints besitzen zwei Funkmodule: Auf einem stellen sie das WLAN für die Clients bereit, auf dem anderen läuft das Mesh. Mesh-Points mit nur einem Funkmodul sind nur dazu da, die Reichweite des Netzwerks zu erhöhen. Mesh-Portals besitzen ein Funkmodul und eine Netzwerkschnittstelle: Sie sind dazu da, die Daten aus dem Mesh ins LAN zu übertragen. Diese drei Funktionen werden heutzutage in ein Gerät integriert: Die untersuchten Mesh-Router besaßen allesamt zwei WLAN-Schnittstellen und eine LAN-Schnittstelle. Somit kann ein Gerät entweder für eine Funktion konfiguriert werden oder alle Funktionen gleichzeitig erfüllen. (siehe Abbildung 12)

Die Anforderungen an das Mesh sind folgende:

- Es soll sich eigenständig aufbauen und verwalten können.
- Für die WLAN-Übertragung sollte die günstigste Verbindungsstrecke gewählt werden. Hierbei spielen die Bandbreite, die Anzahl der Hops (Anzahl der Zwischenstationen), die Latenz und die Anzahl von Übertragungsfehlern eine Rolle.
- Das Mesh soll selbstheilend und redundant sein: Beim Ausfall eines Knotens sollen die Nutzdaten über eine andere Route umgeleitet werden.
- Das Routing soll auf der MAC-Ebene (Layer 2) erfolgen.[53]

[51] Airberry WLAN, Seite 19
[52] Vgl. Rech, Seite 57
[53] Rech, Seite 57

Routingprotokolle, die diese Anforderungen erfüllen, funktionieren ähnlich wie das Kinderspiel „Stille Post“: Durch das Verschicken von Testpaketen wird die Qualität einer Route ermittelt. Für die Datenübertragung wird die Route gewählt, bei der am wenigsten Fehler zu erwarten sind. Die Funktionsweise des Routingprotokolls BATMAN wird im Kapitel 5.1.4 beschrieben.

Großer Nachteil eines Mesh-Netzwerks ist die starke Begrenzung der Datenrate: Solange Zwei Mesh-Teilnehmer direkt miteinander kommunizieren kann die maximal mögliche Datenrate der Funkverbindung genutzt werden. Sobald ein Mesh-Teilnehmer allerdings mit zwei Teilnehmern auf dem gleichen Funkmodul kommuniziert muss die Datenrate pro Verbindung halbiert werden. Dieser Umstand kann vermieden werden, indem weitere Funkmodule genutzt werden.

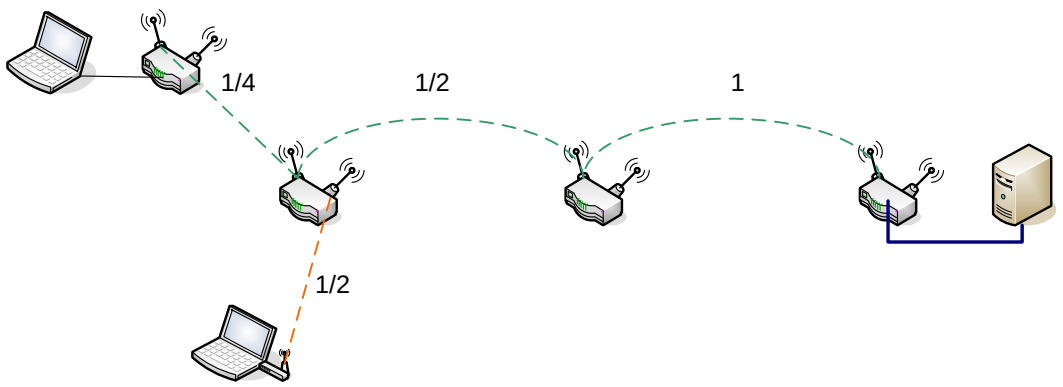


Abbildung 12: Bei jedem Hop halbiert sich die Datenrate

Der große Vorteil einer WLAN-Lösung, die vollständig auf Mesh basiert ist, dass alle Teilnehmer gleichberechtigt sind. Das bedeutet:

- Ein Mesh-Klient wird vollständig in die Mesh-Verwaltung eingebunden
- Sobald sich das Mesh selbständig aufgebaut hat, findet kein Authentifizierungs- und Schlüsselmanagement mehr statt, auch bei Umschaltung der Routen

Dadurch ist ein enormer Zeitvorteil gegenüber einem klassischem ESS zu erwarten.

5 Hauptteil - Arbeitsumgebung

5.1 WLAN Infrastruktur bei CodeOne

5.1.1 CodeOne WLAN ESS

Damit bei CodeOne drahtlos gearbeitet werden kann, gibt es ein ESS, dass aus drei Aruba IAP 105 besteht. Zwei der drei AP sind in der ersten Etage untergebracht, der dritte steht im Erdgeschoss. Somit kann eine Durchdringung des ganzen Gebäudes bis in den Keller erreicht werden. Die IAPs arbeiten auf 2.4 GHz und auf 5 GHz. Die Mesh-Funktion ist deaktiviert, stattdessen sind die APs über Ethernet an das Firmennetzwerk angeschlossen und können darüber miteinander kommunizieren. Die IAPs verwalten selbstständig die Kanäle und die Sendeleistung.

5.1.2 Controllerbasiertes WLAN von Aruba

Um ein großes drahtloses Firmennetzwerk verwalten zu können, reicht Consumer-Technik nicht mehr aus. Stattdessen werden sämtliche Accesspoints zentral gesteuert. Dafür kommen sog. WLAN-Controller zum Einsatz. Mittels Controller können umfassende Konfigurationen vorgenommen werden. Der Aruba 650 Mobility Controller beinhaltet beispielsweise neben dem obligatorischen WLAN Controller eine Firewall, einen 8-Port Ethernet-Switch, einen File- und Printserver und kann VPN Dienste bereitstellen.[54] Zudem können im WLAN VLANs und Nutzergruppen verwaltet werden und die Authentifizierung kann über einen RADIUS-Server erfolgen. Sämtliche Einstellungen können in Gruppenprofilen gespeichert werden. Ein neu angeschlossener AP muss also nur noch einer Gruppe zugeordnet werden und erhält alle Eigenschaften des entsprechenden Profils. Mittels Controller können theoretisch unendlich große WLAN Netze realisiert werden. Zudem stehen Analyse-Werkzeuge zur Verfügung, um den Netzwerk-Traffic zu überwachen. Für CodeOne bietet eine controllerbasierte WLAN-Lösung den komfortablen Vorteil, dass APs im Vorhinein konfiguriert werden können. Soll bei einer Veranstaltung WLAN bereitgestellt werden, müssen die APs also nur noch angeschlossen werden.

[54] Aruba 650 Controller Data-Sheet

Abbildung 13: Aruba 650 Mobility Controller

Die Aruba-WLAN-Lösungen passen sich dynamisch an die Auslastung auf den beiden Frequenzbändern 2.4 GHz und 5 GHz an: Über die WLAN-Module der Accesspoints kann die Auslastung auf den Frequenzbändern gemessen werden. Die Messergebnisse werden von dem sogenannten „Adaptive Radio Management“ (ARM) ausgewertet, bei Bedarf werden automatisch Änderungen in der WLAN Konfiguration vorgenommen. So können Kanäle und Sendeleistung angepasst werden. Wenn ein WLAN auf beiden Frequenzbändern 2.4 und 5 GHz arbeitet, können zudem die Clients dynamisch verteilt werden: Unterstützt ein WLAN-USB-Stick zum Beispiel 2.4 GHz und 5 GHz, kann er vom ARM auf das 5 GHz-Band gezwungen werden, damit auf dem ohnehin sehr vollen 2.4 GHz-Band nur die Clients verbleiben, die kein 5 GHz unterstützen.

5.1.3 Aruba IAPs

Da der Konfigurationsaufwand für controllerbasierte WLAN-Lösungen relativ groß ist, drängen immer mehr „Instant Accesspoints“ auf den Markt, welche sich weitestgehend selbst erkennen und verwalten können. Für Tests standen IAPs der Serie 105 zur Verfügung. Diese sind im Gegensatz zur controllerbasierten Lösung stark abgerüstet, bieten jedoch die Möglichkeit ein Mesh aufzubauen. Der Aufbau der Selbstverwaltung erfolgt bei den IAPs IP-basiert, entweder mit Hilfe eines DHCP-Servers oder manuell konfigurierter IP-Adressen.

Abbildung 14: Aruba IAP 105

Für den Aufbau eines ESS wird ein IAP an einen DHCP Server angeschlossen und erhält eine IP-Adresse. Daraufhin übernimmt dieser AP die Controllerfunktion im WLAN: Über die zugewiesene IP-Adresse ist ein „Virtual Controller“ erreichbar, über den das WLAN konfiguriert werden kann. Jeder weitere angeschlossene IAP erkennt daraufhin den Controller-IAP als „Master“ an und wird zum „Slave“. Seine MAC-Adresse und die zugewiesene IP-Adresse werden im Virtual Controller aufgeführt. Auch die IAP 105 unterstützen ARM.

5.1.4 Airberry

Abbildung 15: Airberry: Mobiler Accesspoint

Um die Funktionsweise ihres Mesh-Netzwerkes zu testen, stellte die Firma Airberry freundlicherweise fünf Mesh-Router des Typs 2oA zur Verfügung. Jeder Router besitzt 3 physikalische Interfaces: 1x WLAN auf 2.4 GHz, 1x WLAN auf 5 GHz und 1x Ethernet. Die WLAN-Interfaces unterstützen den 11g bzw. 11a Standard, damit sind Bruttodatenraten von 54 MBit/s möglich (siehe Tabelle 2). Praktisch reduziert sich der Datendurchsatz jedoch um die Hälfte.[55] Zudem gibt es 2 virtuelle Interfaces, das Mesh

[55] Vgl. Rech, Seite 409

und die Bridge: Über das Mesh funktioniert die Interne Kommunikation der Router über das Routingprotokoll, in der Bridge werden die Nutzdaten wieder an externe Geräte ausgegeben. Bemerkenswert ist, dass völlig frei konfiguriert werden kann, welches physikalische Interface gerade zu welchem virtuellen Interface gehört.

	Mesh: Intern	Verbindung	Bridge: Extern
Interfaces	WLAN 1: 2.4 GHz		WLAN 1: 2.4 GHz
	WLAN 2: 5 GHz		WLAN 2: 5 GHz
	Ethernet		Ethernet

Abbildung 16: Matrix: Verschaltung der Module in der Herstellerkonfiguration

Das Mesh funktioniert als Gleichwellennetz, daher ist es für den Aufbau des Mesh notwendig, dass die entsprechenden WLAN-Interfaces an allen Routern dieselbe SSID, dieselbe Verschlüsselung und denselben Kanal benutzen. Als Routingprotokoll wird Batman-Advanced (B.A.T.M.A.N = Better Approach To Mobile Adhoc Networks) genutzt. Im Gegensatz zu vielen anderen Routingprotokollen basiert Batman-adv auf Layer 2 des OSI-Modells[56]: Die Idee hinter Batman-adv ist, dass die Informationen über die besten Routen, also die besten Ende-zu-Ende Verbindungen durch das gesamte Mesh Netzwerk geflutet werden: Dabei überträgt jede einzelne Node (Originator) eine Broadcast-Nachricht (sog. Originator Message = OGM) an seine Nachbarn. Die Nachbarn versenden diese OGM weiter an andere Nodes, bis das gesamte Netzwerk diese OGM erhalten hat. Die OGM‘s sind sehr klein und bestehen lediglich aus der MAC-Adresse des Auftraggebers (Originator), der MAC-Adresse der aktuell übertragenden Node, einer TTL Information und einer Sequenznummer.

Wenn eine schlechte physikalische Verbindung zwischen zwei Nodes besteht, treten bei der Übertragung einer OGM logischerweise hohe Paketverluste und Verzögerungen auf. Bei einer guten Verbindung sind diese Paketverluste und Verzögerungen geringer. Jede einzelne Node kann anhand dessen aus einer Vielzahl von empfangenen OGM’s den am besten erreichbaren Nachbarn ermitteln. Nur die OGM dieses Nachbarn wird weiterverschickt, alle anderen OGM’s werden verworfen. So kann für jede einzelne Node die beste Route ermittelt werden.

Das Fluten mit Informationen durch das Mesh findet in regelmäßigen Zeitabständen (OGM-Interval) statt: Ändert sich eine Route, wird das beim nächsten Fluten mitgeteilt. Durch die Vielzahl der möglichen Routen herrscht Redundanz.

[56] Open Mesh

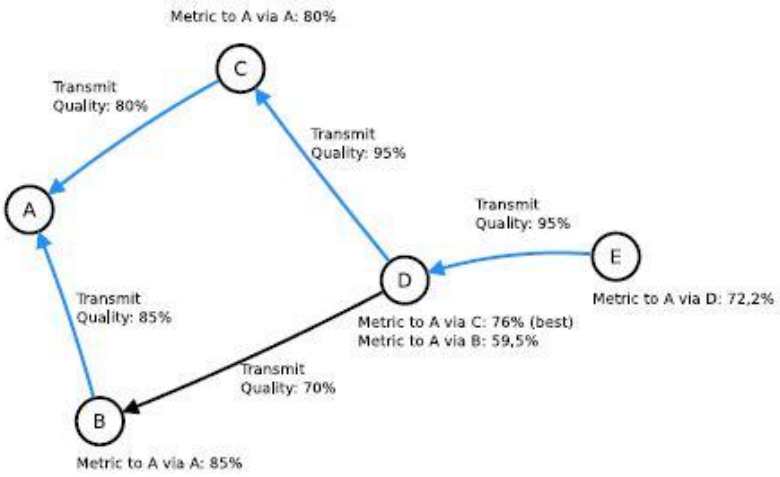


Abbildung 17: Fluten und Routenbildung[57]

Die Metrik, also die Aussage über die Leistungsfähigkeit einer Route bis zum nächsten Nachbarn wird mit einer 8 Bit großen Zahl dargestellt und kann somit Werte zwischen 0 und 255 annehmen. In die Metrik fließen eine ganze Menge Faktoren ein. Ausschlaggebend sind jedoch Sendeleistung und Anzahl der Hops. Durch den Einsatz einer Ethernetverbindung zwischen zwei Routern im Mesh kann die Metrik auf ein Maximum gesteigert werden. Zudem finden keine Hops mehr statt, dadurch kann eine Begrenzung der Datenrate vermieden werden.

5.1.5 Clients

Bei den zur Verfügung stehenden Clients handelt es sich um die internen WLAN-Karten der Laptops, zum Beispiel eines Acer 5750G mit einer b,g,n fähigen Broadcom-WLAN-Schnittstelle. Diese arbeitet allerdings nur auf 2.4 GHz. Für weitere Tests u.a. auf 5GHz stehen mehrere WLAN-USB-Sticks (Fritz WLAN USB Stick N, Netgear WNDA 3100) sowie Netzwerkadapter (Netgear WNCE 3001) bereit. Besonderheit bei den Netzwerkadaptern ist, dass sie keine Treiberinstallation voraussetzen, und alle Einstellungen über ein Web-Interface vorgenommen werden. Der große Vorteil dieser Netzwerkadapter liegt darin, dass sie an einem Computer vorkonfiguriert werden können, um dann zum Beispiel an einen Fernseher mit Netzwerkschnittstelle angeschlossen werden können. Nachteil bei dem WNCE 3001 ist die geringe Anzahl an Konfigurationsmöglichkeiten. Der Netgear WNDA 3100 dagegen lässt sich am besten

[57] Airberry_wireless_mesh

konfigurieren. Der eingebaute Broadcom BCM4323 Chipsatz bietet zwei Parameter, um Roaming gezielt zu beeinflussen: Der WLAN-USB-Stick kann in Windows unter Gerätemanager/Netzwerkadapter aufgerufen werden. Unter „Erweitert“ lassen sich die Parameter „Roaming Decision“ und „Roam Tendency“ aufrufen. „Roaming Decision“ beeinflusst, bei welcher ermittelten Sendeleistung der USB anfängt zu scannen. „Roam Tendency“ dagegen beeinflusst die Auswahl des nächsten APs in Bezug auf Sendeleistung. Um Handover zu optimieren sollten die Werte auf „Optimize Bandwith“ bzw. „Aggressive“ eingestellt werden Dadurch fängt der USB Stick an zu scannen wenn zum aktuellen AP eine Sendeleistung von kleiner -60dBm ermittelt wird, (Standard -70 dBm) bzw. wechselt zu nächsten AP wenn zu diesem ein Unterschied in der Sendeleistung von größer 10 dB gemessen wird (Standard 20 dB).[58]

Abbildung 18: Externe Adapter: Netgear WNCE 3001, Fritz N WLAN Stick, Netgear WNDA 3100

[58] Linksys.info

5.2 Ableitung von Testszenarien für schnellen Handover

5.2.1 Controllerbasiertes WLAN von Aruba: ESS

Mit den Aruba Komponenten Controller 650 und zwei AP 105 kann ein ESS realisiert werden, das sowohl auf 2.4 GHz als auch auf 5 GHz arbeitet. Das WLAN sollte über PSK mit AES verschlüsselt sein und hohe Datenraten nach dem 802.11n Standard unterstützen, die bei Aruba „High Troughput Layer“ genannt werden. Außerdem sollten Spezifikationen vorgenommen werden, die schnelles Roaming unterstützen. Das sind zum einen die in 802.11i definierten „PMKSA-Cashing“ und „Pre-Authentication“ die bei Aruba als „Opportunistic Key Cashing“ bzw. „Multi Association“ umgesetzt werden. Außerdem kann ein Trick angewendet werden: Indem die Übertragung von kleinen Bandbreiten, zum Beispiel Bandbreiten unter 11 MBit/s verboten werden, wird die Reichweite der APs stark begrenzt und der Client sollte dadurch gezwungen werden, früher zu wechseln. Zusätzlich sollte Sendeleistung der APs reduziert werden. Zum Vergleich sollte Handover in einem unverschlüsselten Netz betrachtet werden.

Opportunistic Key Caching	By default, the 802.1x authentication profile enables a cached pairwise master key (PMK) derived via a client and an associated AP and used when the client roams to a new AP. This allows clients faster roaming without a full 802.1x authentication. Uncheck this option to disable this feature. **Note:** Make sure that the wireless client (the 802.1x supplicant) supports this feature. If the client does not support this feature, the client will attempt to renegotiate the key whenever it roams to a new AP. As a result, the key cached on the controller can be out of sync with the key used by the client.

Abbildung 19: Screenshot Aruba OKC[59]

Multi Association	Enables or disables multi-association for this virtual AP. When enabled, this feature allows a station to be associated to multiple APs. If this feature is disabled, when a station moves to new AP it will be de-authorized by the AP to which it was previously connected, deleting station context and flushing key caching information. Important things to know when using the Multi Association feature: • When enabled, the system allows multiple associations per client. If the maximum number of clients allowed per AP is limited to a small number there is a risk of increased association failures. • If a client has multiple associations, it may not do active scanning before roaming event which could result in it not being associated to nearest AP. • Multiple associations may result in more frequent roaming.

Abbildung 20: Screenshot Aruba Multi Association[60]

59 Aruba: Seite 302
60 Aruba: Seite 153

5.2.2 Aruba IAPs: Mesh

Für den Aufbau eines Mesh wurden 2 IAPs (AP82 und AP90) an einen kleinen Cisco-Router angeschlossen, der als DHCP-Server fungierte. Nachdem die IP-Adressen vergeben worden waren und ein IAP (AP82) als Virtual Controller fungierte, konnte die LAN-Verbindung von AP90 zum Cisco-Router gekappt werden. Die Aruba-Logik passte daraufhin die Kanäle automatisch an und baute ein Mesh auf. Für die Tests wurden 2 WLANs mit jeweils WPA2 Authentifizierung und AES Verschlüsselung konfiguriert: IBC 2 stellte WLAN auf 2.4 GHz bereit und IBC 5 stellte WLAN auf 5 GHz bereit. Der Aufbau des Mesh funktionierte davon unabhängig, nämlich auf 5 GHz auf Kanal 44+.

Testsetup 2+1

Der Test 2+1 wurde mit dem Broadcom WLAN-USB-Stick durchgeführt.

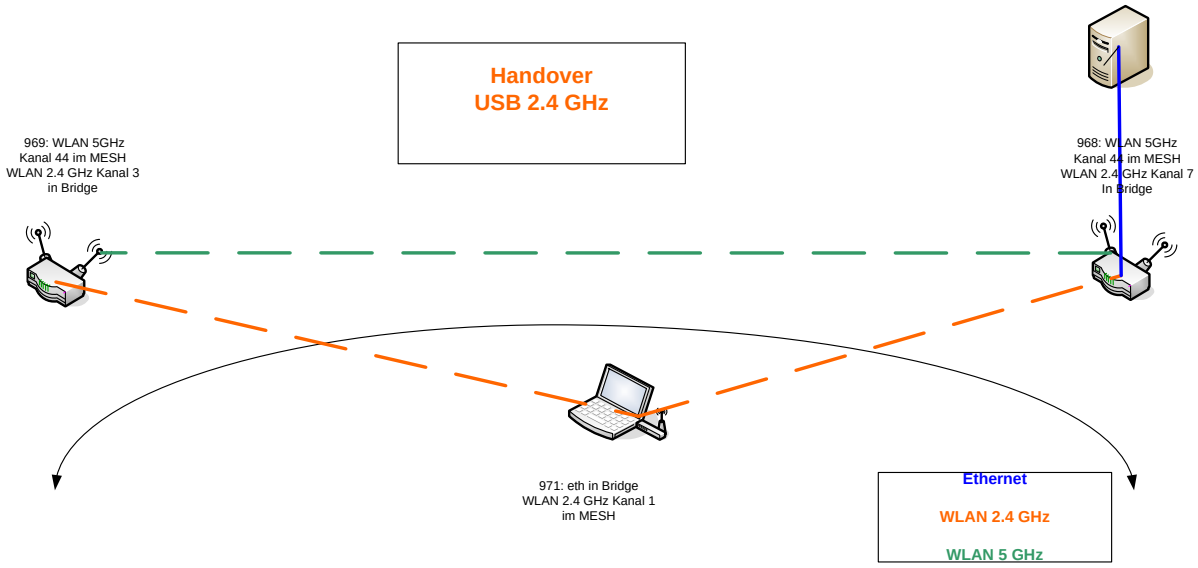
Testsetup 3 APs

Es ist möglich, die IAPs für Wireless Bridging zu konfigurieren. Dazu muss die Option „ETH0-Überbrückung“ unter Uplink aktiviert werden. So kann die Weitergabe der Daten von einem Laptop ins Mesh anstatt über ein WLAN-Modul über die Netzwerkschnittstelle erfolgen und der Accesspoint kann als mobiler Mesh-Client genutzt werden.

5.2.3 Airberry: Mesh

Durch die großzügigen Konfigurationsmöglichkeiten bei den AirBerry Mesh-Accesspoints ist eine Vielzahl von Testszenarien für Handover möglich. Zum einen sollte die Verbindung von zwei Mesh-Accesspoints und einem „normalen“ Client, wie einem WLAN-USB Stick getestet werden. (2+1) Zum anderen sollte die Leistungsfähigkeit des Mesh in Bezug auf Handover genau untersucht werden. Hier besteht die Möglichkeit, einen dritten Mesh-Accesspoint über Ethernet direkt mit einem Laptop zu verbinden und als mobilen Client zu nutzen. (3APs)

Testsetup 2+1



968/969	Mesh: Intern	Verbindung	Bridge: Extern
Interfaces	WLAN 1: 2.4 GHz		WLAN 1: 2.4 GHz
	WLAN 2: 5 GHz		WLAN 2: 5 GHz
	Ethernet		Ethernet

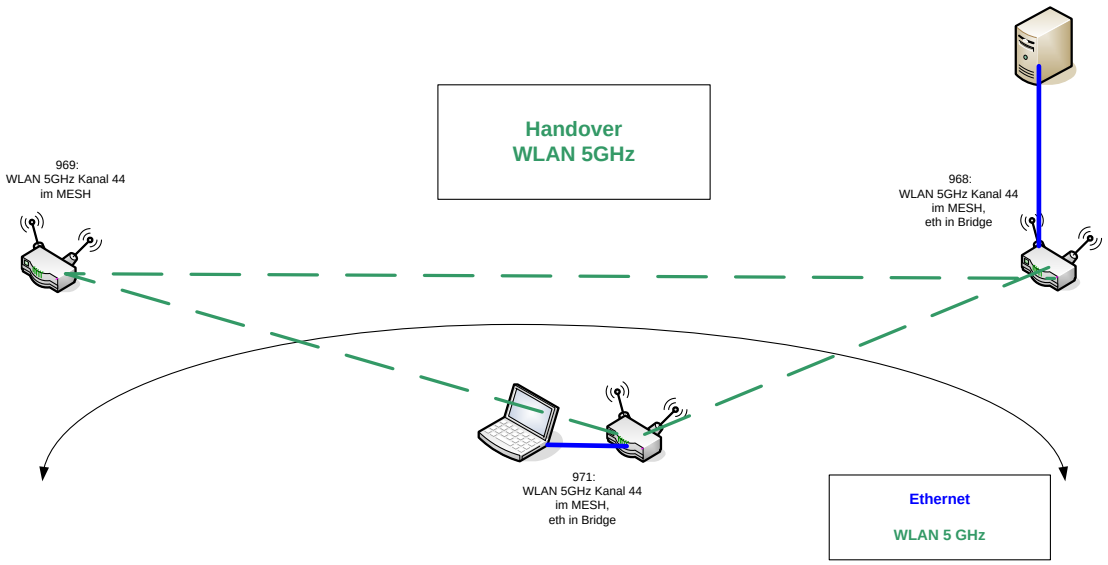
Abbildung 21: Testszenario 2+1: Mesh-Netzwerk mit einem WLAN USB Client

Beim Testszenario 2+1 können wiederum die Interfaces unterschiedlich konfiguriert werden. Auf Jeden Fall ist es aber bei der Nutzung eines WLAN USB Sticks notwendig, eins von zwei WLAN-Interfaces an beiden Routern mit der Bridge zu verknüpfen, da ein externer USB Stick das BATMAN-Protokoll, dass die Router für die Kommunikation nutzen schlichtweg nicht verarbeiten kann.

Somit kann sowohl ein Setup aufgebaut werden, dessen Mesh WLAN auf 5 GHz nutzt und die Nutzdaten auf 2.4 GHz ausgibt, als auch ein Setup, dessen Mesh WLAN auf

2.4 GHz nutzt und die Nutzdaten auf 5 GHz ausgibt. Zudem muss Ethernet in der Bridge konfiguriert werden, damit die Daten über Kabel an den Decoder ausgegeben werden können.

Testsetup 3APs



968/969/971	Mesh: Intern	Verbindung	Bridge: Extern
Interfaces	WLAN 1: 2.4 GHz		WLAN 1: 2.4 GHz
	WLAN 2: 5 GHz		WLAN 2: 5 GHz
	Ethernet		Ethernet

Abbildung 22: Testszenario 3APs: 3 Airberry-Router in der Standardkonfiguration

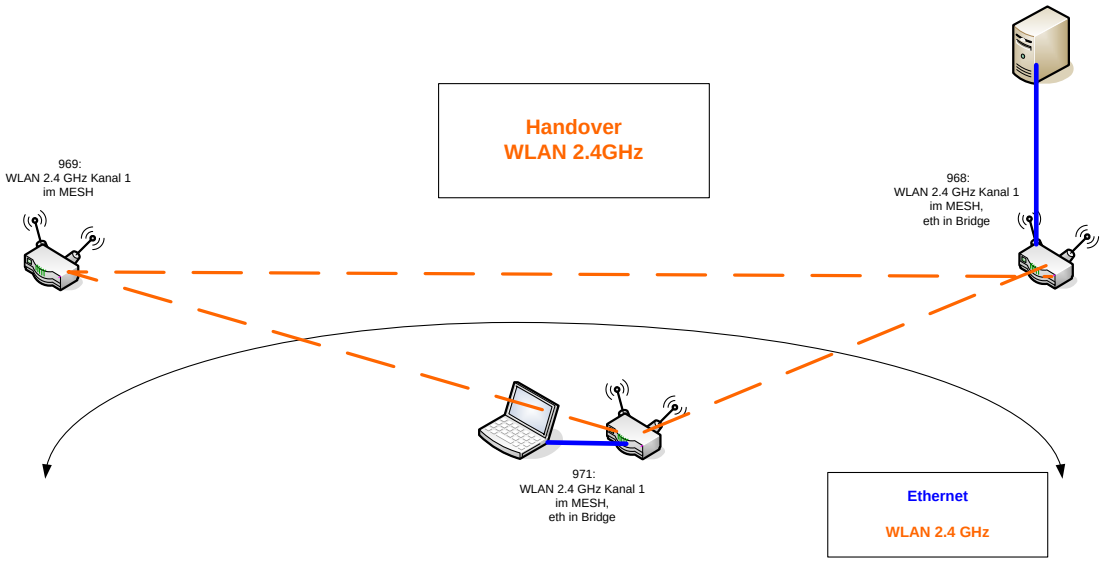
Beim Testszenario 3APs kommunizieren die 3 Mesh-Router über das 5 GHz-Modul miteinander, zudem wird das Ethernet-Modul in der Bridge gebraucht, um die Nutzdaten vom Encoder zum Airberry-Client zu übergeben und sie am Ende wieder an den Decoder auszugeben. Das zweite WLAN-Modul in der Bridge wird für den Handover nicht gebraucht.

Bei den Tests stellte sich sehr schnell heraus, dass Handover in der Standardkonfiguration nicht zuverlässig funktioniert. Anhand des Testskripts konnten Ping-Ausfälle über mehrere Sekunden beobachtet werden, zudem brach die Datenrate stark ein (siehe Kapitel 7.3.2).

Daraufhin wurden folgende Lösungsansätze entwickelt:

- Das OGM-Intervall, also das Intervall, mit dem die Router Informationen über die Nachbarschaftserkennung und Routenfindung austauschen, wurde verkürzt.

- Die Mesh Kommunikation wurde von 5 GHz auf 2.4 GHz umgestellt. (siehe Abbildung 23)

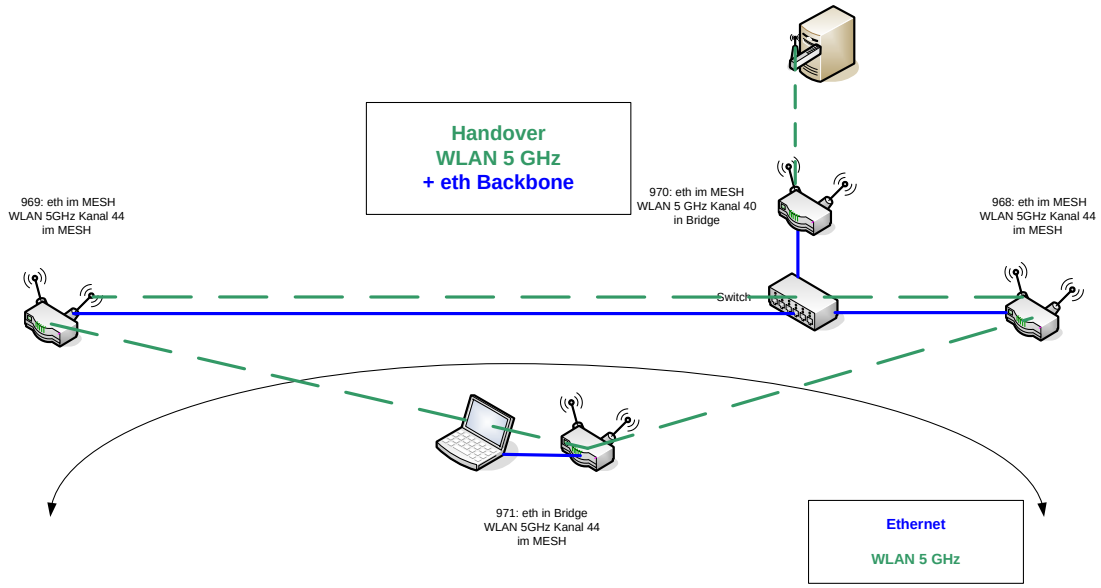


968/969/971	Mesh: Intern	Verbindung	Bridge: Extern
Interfaces	WLAN 1: 2.4 GHz		WLAN 1: 2.4 GHz
	WLAN 2: 5 GHz		WLAN 2: 5 GHz
	Ethernet		Ethernet

Abbildung 23: Matrix Setup 2: Mesh auf 2.4 GHz, Bridge auf 5GHz

- Der Mesh-Backbone, d.h. die beiden stationären Router wurden mit Ethernet miteinander verbunden.

Dadurch, dass das Ethernet-Modul Teil der Mesh-Kommunikation war, konnte es nicht mehr verwendet werden, um die Nutzdaten über Kabel an den Decoder auszugeben. Hier hätte ein Mesh-Router mit zwei Ethernet-Modulen Abhilfe schaffen können, dieser war aber in der Kürze der Zeit nicht lieferbar. Stattdessen wurde ein vierter Mesh-Router (970) verwendet, dessen Ethernet-Modul im Mesh und das 5GHz WLAN-Modul auf einem separaten Kanal in der Bridge konfiguriert war Für die Weiterleitung zum Decoder wurde eine zweite WLAN-Verbindung mit USB-Stick genutzt.



968/969	Mesh: Intern	Verbindung	Bridge: Extern
Interfaces	WLAN 1: 2.4 GHz		WLAN 1: 2.4 GHz
	WLAN 2: 5 GHz		WLAN 2: 5 GHz
	Ethernet		Ethernet

971	Mesh: Intern	Verbindung	Bridge: Extern
Interfaces	WLAN 1: 2.4 GHz		WLAN 1: 2.4 GHz
	WLAN 2: 5 GHz		WLAN 2: 5 GHz
	Ethernet		Ethernet

970:	Mesh: Intern	Verbindung	Bridge: Extern
Interfaces	WLAN 1: 2.4 GHz		WLAN 1: 2.4 GHz
	WLAN 2: 5 GHz		WLAN 2: 5 GHz
	Ethernet		Ethernet

Abbildung 24: Testsetup Ethernet-Backbone 5 GHz

5.3 Werkzeuge

5.3.1 Streaming Produkte

Die Arbeitsumgebung für die Handover-Tests wird im Folgenden dargestellt. Bei IP-basierter Live-Videoübertragung wird ein Kamera-Signal in MPEG-Container verpackt, über ein IP-Netz transportiert und an einer Gegenstelle wieder entpackt und ausgegeben. Hierfür standen ein Laptop mit einer Webcam und der CodeOne Encoder-Software, sowie eine Workstation mit CodeOne Decoder-Software sowie einem lokalen Wowza-Media-Server zur Verfügung.

Encoder

Abbildung 25: CodeOne Encoder im Streaming Mode

Der CodeOne Encoder codiert das Kamerasignal in H264. In einem User Interface können hierfür alle nötigen Parameter eingestellt werden. In den Settings können Video- und Audioeingänge, Videoqualität (Format, Auflösung, Bitrate) sowie Zieladresse des Streams und Transportprotokoll angegeben werden. Außerdem kann die automatische Anpassung der Datenrate an- oder ausgestellt werden. Anschließend kann der Encoder in den Streaming-Modus versetzt werden und der Stream kann über die Play-Taste gestartet werden. Bei der Wahl des Streamingprotokolls ist zu beachten, dass RTMP entweder einen Flash-Player für Webcast oder einen Wowza Media Server für Unicast an der Gegenstelle benötigt.

Decoder

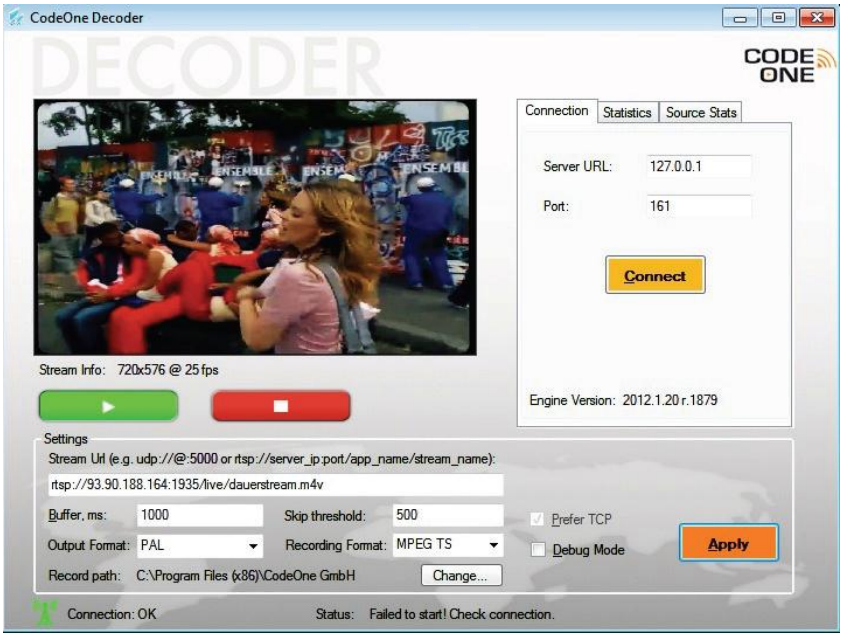


Abbildung 26: CodeOne Decoder

Der Decoder ist Gegenstelle für die Wiedergabe des Videostreams. Hier können weitere Einstellungen vorgenommen werden, die die Stabilität des Streams beeinflussen. Der wichtigste Parameter ist der Empfangspuffer und damit die Latenz der Verbindung. Je länger der Empfangspuffer eingestellt wird, desto stabiler ist der Videostream. Typische Werte sind hier Latenzen zwischen 1-3 Sekunden. Zudem kann der Stream als Videodatei mitgeschnitten und abgespeichert werden.

Zu beachten ist, dass diese Produkte Encoder und Decoder im Normalfall mit einer Videokarte verbaut werden, um professionelle Videoformate wie SDI annehmen oder ausgeben zu können, bei den Tests wurde jeweils eine Stand-Alone Variante verwendet.

Wowza

Der Wowza Media Server ist eine JAVA-Application, mit der es möglich ist, dass proprietäre und eigentlich für Webcast vorgesehene RTMP von Adobe in ein anderes Protokoll wie RTP zu wandeln. Dadurch kann eine Punkt-zu-Punkt Verbindung zum Decoder aufgebaut werden.

5.3.2 Konfigurations- und Messtools

Webinterface: Aruba OS 6.1

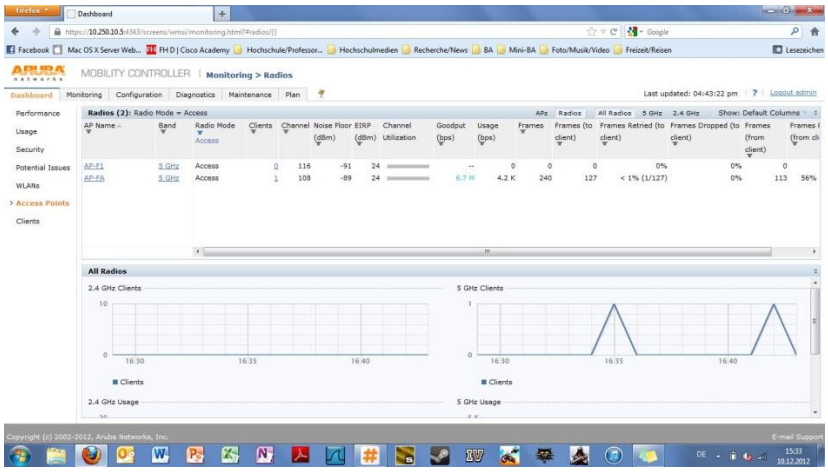


Abbildung 27: Screenshot Aruba OS 6.1

Die Konfiguration des Aruba 650 Controllers erfolgt in einem Betriebssystem-ähnlichen Webinterface, dem Aruba OS, das mittlerweile in der Version 6.1 verfügbar ist.

Webinterface: Airberry Configurator

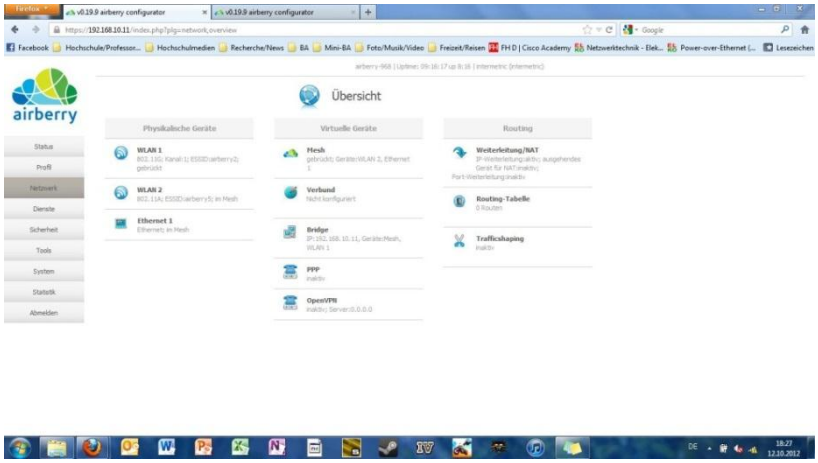


Abbildung 28: Screenshot Webinterface Airberry: Netzwerk

Die Airberry Mesh-Router können über ein Webinterface konfiguriert werden. Das Webinterface erzeugt eine XML-Datei, diese enthält sämtliche WLAN-Parameter und wird mit dem entsprechenden Befehl „Profil aktivieren“ geladen.

Putty

Zudem gibt es die Möglichkeit, die Airberry-Router über einen SSH-Klienten auf die Shell eines Routers zuzugreifen. So kann eine Vielzahl von Daten abgefragt werden. Als SSH-Klient wurde Putty gewählt.

JPerf

JPerf ist die grafische Oberfläche für das Konsolentool IPerf, Vorteil von JPerf gegenüber IPerf ist neben der einfachen Bedienung vor allem die Ausgabe der Ergebnisse als Diagramm. Mit JPerf kann die Leistungsfähigkeit eines Netzwerks ermittelt werden. Dafür werden Transportströme generiert, die von einem Client (Rechner A) über das Netzwerk zu einem Server (Rechner B) übertragen werden. Als Protokoll stehen sowohl TCP als auch UDP zur Verfügung. Die Protokoll-Parameter lassen sich anpassen. Großer Nachteil von JPerf ist, dass TCP-Datenströme das Netzwerk immer maximal auslasten, eine Begrenzung der Bitrate ist nur bei UDP möglich.

InSSIDer

Die Freeware InSSIDer scannt alle WLAN-Netze im Empfangsbereich. Es überprüft deren Empfangsstärke, ermittelt die Sicherheitseinstellungen und weitere Details. So wird beispielsweise der Sendekanal erfasst, die MAC-Adresse oder der genaue Standort. InSSIDer kann auch dazu benutzt werden, die Sendeleistung zu bestimmen. Die ermittelten Werte sind zwar nicht exakt, Pegelunterschiede können aber sehr gut festgestellt werden.

Netmeter

Mit der Freeware Netmeter kann der eingehende und ausgehende Traffic einer Netzwerkkarte als Graph angezeigt werden. Hierbei lassen sich die Achsen frei skalieren.

Capture Solution

Mit Capture Solution lässt sich der Desktop eines Rechners inklusive Ton aufzeichnen. Die Videodaten können zum Beispiel als avi-Datei abgespeichert werden.

6 Hauptteil - Testverfahren/ Abläufe

Um die Leistungsfähigkeit der einzelnen Systeme in Bezug auf Handover vergleichen zu können, ist es wichtig, die Testabläufe so weit wie möglich zu vereinheitlichen. Trotz großer Unterschiede in der Arbeitsweise und der Konfiguration zwischen Aruba und Airberry sollte stets nachvollzogen werden können, ob ein Wechsel zwischen zwei APs (also Handover) stattgefunden hat und ob dieser Wechsel Einfluss auf die Datenrate genommen hat.

Arbeitsschritte für ein erfolgreiches Testverfahren sind im Einzelnen:

Schritt 1:

Überprüfung der Arbeitsumgebung auf Störungen durch andere WLANs mit InSSIDer

Schritt 2:

Ableitung und Konfiguration der optimalen Kanaleinstellungen bzw. Sendeleistungen für die Teststellung

Schritt 3:

Überprüfung der Einstellungen mit InSSIDer und ggf. Nachbesserungen

Schritt 4:

Teststreaming im Stillstand mit JPerf und Ermittlung des Datendurchsatzes an den verschiedenen Accesspoints: Beim Mesh sollte sich der Datendurchsatz pro Hop um die Hälfte reduzieren (siehe Abbildung 12)

Schritt 5:

Überwachung des Handovers

Die Überwachung darüber, ob tatsächlich ein Wechsel von einem Accesspoint zum nächsten stattfindet oder nicht ist der eigentliche Knackpunkt bei den Tests. Um den Wechsel nachvollziehen und sichtbar machen zu können, muss auf die einzelnen Konfigurationsoberflächen der Hersteller zurückgegriffen werden: Sowohl im Aruba OS 6.1 als auch im Virtual Controller der IAPs sind das die Webinterfaces: Hier werden die MAC-Adressen der Accesspoints im WLAN-Netz angezeigt, zusammen mit den IP-

Adressen der verbundenen Clients. Erfolgt ein Handover wechselt die Anzeige der Client-IP-Adresse von einem Accesspoint zum nächsten. Dieser Wechsel im Webinterface erfolgt allerdings nicht in Echtzeit sondern mit etwa drei Sekunden Verzögerung. Bei dem Testszenario 3APs mit den IAP 105 kann bei Aruba allerdings keine Abfrage des Handoververhaltens erfolgen, da keine Details zur Verbindungsqualität des Mesh angezeigt werden können.

Für die Überwachung der Airberry Mesh-Nodes bei den Tests kann vom Decoder aus eine SSH-Session zu jeweils allen beteiligten Routern aufgebaut werden. Damit ist es möglich ein Skript auszuführen, das regelmäßig Statusinformationen der Router abfragt. Für die Tests waren die Parameter Systemzeit und Ping interessant, um die Erreichbarkeit der Router zu überwachen. Für das 2+1 Testsetup wurden zudem alle MAC-Adressen von Non-Mesh-Clients abgefragt. Damit konnte nachvollzogen werden mit welchem Router der USB WLAN Stick gerade verbunden ist. Bei dem 3APs Testsetup erfolgte eine Überwachung der Nachbarschaftserkennung: So konnten Aussagen über die Routenfindung und über die Leistungsfähigkeit des Mesh getroffen werden.

- Befehl für die 2+1 Überwachung:

```
while [ 1 -eq 1 ]; do clear ; date ; cat "/proc/net/batman-
adv/transtable_local" ; ping -c 1 192.168.10.12; sleep 1; done
```

- Befehl für die 3APs Überwachung:

```
while [ 1 -eq 1 ]; do clear ; date ; cat "/proc/net/batman-
adv/originators" ; ping -c 1 192.168.10.12; sleep 1; done
```

Bei den drei beteiligten Routern muss nur noch die IP-Adresse angepasst werden.

Schritt 6:

Streaming in Bewegung mit JPerf

Um Aussagen darüber zu bekommen, ob sich das aktuelle Testsetup für Videostreaming in Bewegung tatsächlich eignet bzw. welche Datenraten tatsächlich möglich sind, ist es sinnvoll, das Verhalten des WLAN-Netzes bei maximalem Datendurchsatz (Stresstest) einerseits und bei konstanter, geringer Datenraten andererseits zu untersuchen. Über die Generierung von TCP-Datenströmen mit JPerf wird das Netz maximal ausgelastet. Dadurch kann eine durchschnittliche Datenrate ermittelt werden, zudem können Aussagen über das Handoververhalten getroffen werden. Bei Tests mit UDP mit einer konstanten Datenrate kleiner der vorher ermittelten Durchschnittsdaten-

rate kann das Handoververhalten überprüft werden. Hier wurde eine Datenrate von 5 MBit/s gewählt. Kommt es bei den Testergebnissen zu großen Aussetzern der Datenrate, kann ein Test mit Videostreaming verworfen werden.

Schritt 7:

Videostreaming mit CodeOne Software

Weisen die Testergebnisse aus Schritt 6 ein gutes Handoververhalten auf, sollte ein Test mit Videostreaming durchgeführt werden. So kann das Zusammenspiel der drei Softwarekomponenten Encoder, Wowza und Decoder untersucht und eruiert werden, ob sich das Testsetup tatsächlich für Videostreaming eignet.

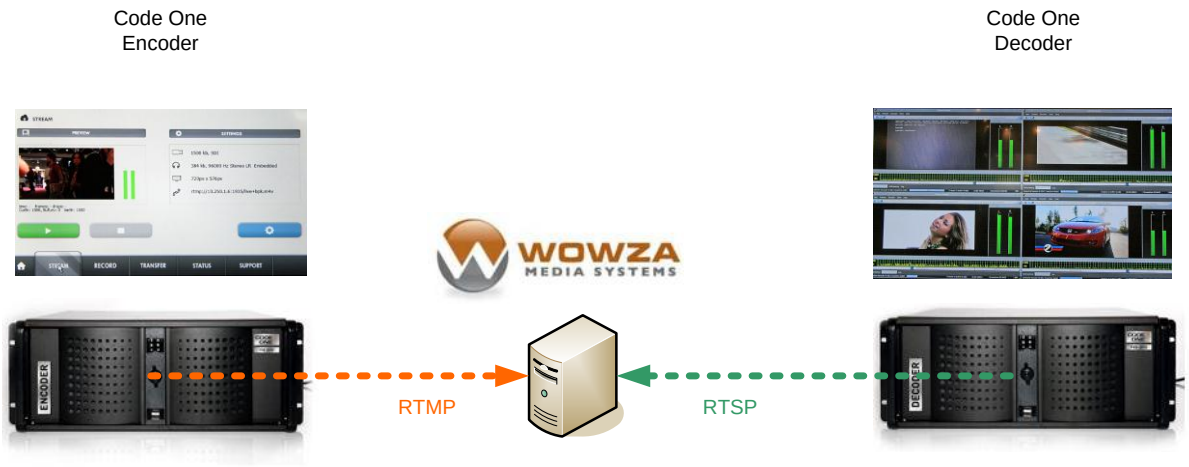


Abbildung 29: Zusammenhang der CodeOne Softwarekomponenten

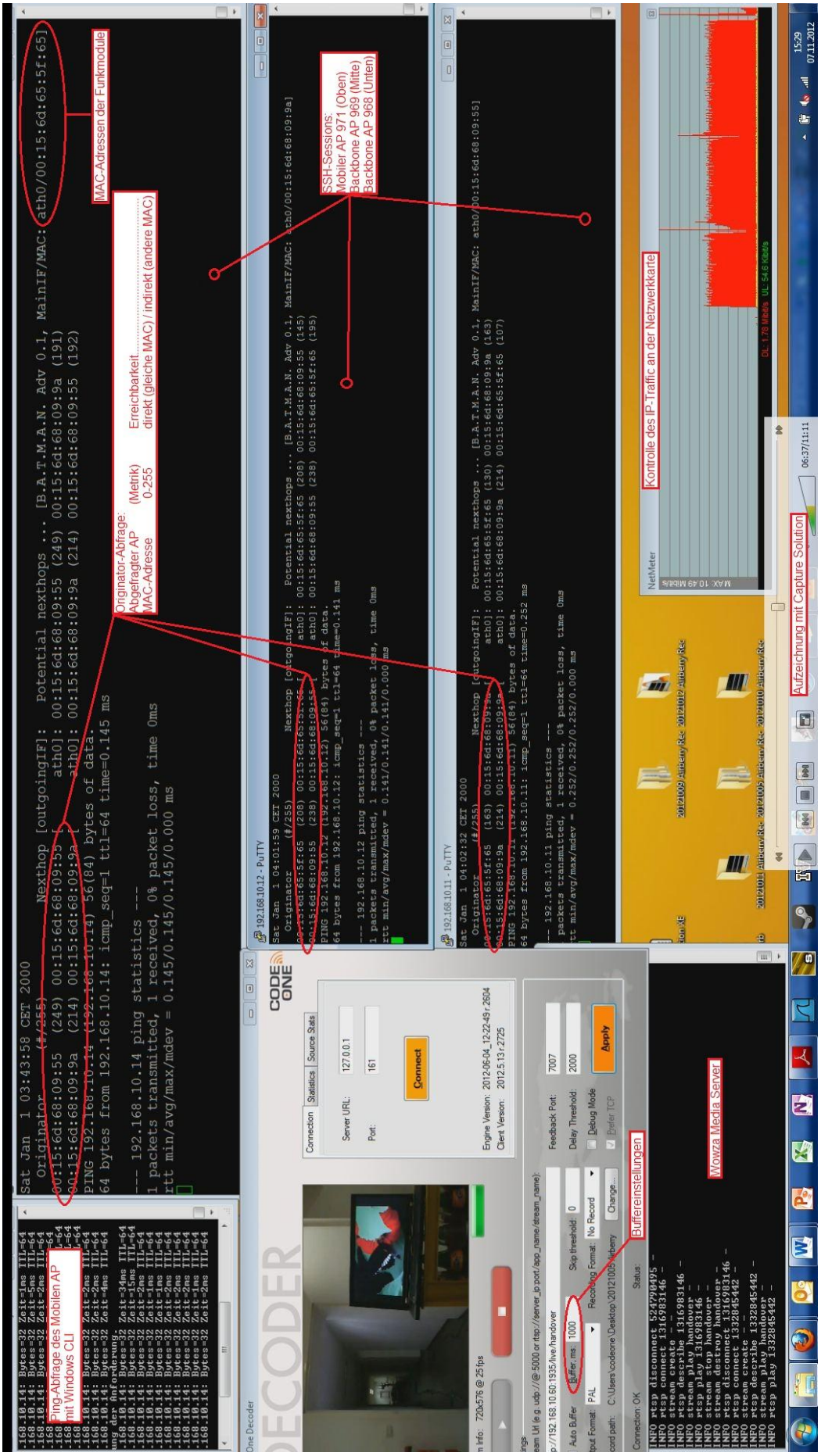
Ein Videosignal einer USB-Webcam wird mit H264 mit einer Auflösung von 720x 576 Pixeln codiert, die Datenrate wird auf 5 MBit/s komprimiert (ohne Bitratemanagement). Als Transportprotokoll wird RTMP gewählt, für den Aufbau einer Punkt-zu-Punkt-Verbindung wird zunächst der Wowza Media Server auf Port 1935 angewählt. Der Wowza Media Server packt die Nutzdaten von RTMP nach RTP um. Der Decoder fragt diesen Stream mit RTSP ab und lädt ihn in den Empfangspuffer. Um möglichst wenig Delay zu erzielen und damit den hohen Anforderungen für eine Liveübertragung gerecht zu werden, sollte der Puffer nicht mehr als 1000ms betragen.

Wichtig bei der Untersuchung ist, wie sich die Stabilität des Videostreams und die Software bei kurzen Aussetzern der Datenrate verhält. Schritt 7 ist der letzte Schritt des Testablaufs. Es können nun konkrete Ergebnisse festgehalten werden, ob das

Handoververhalten einer bestimmten WLAN-Systemlösung im Zusammenspiel mit der CodeOne Software für unterbrechungsfreies Videostreaming geeignet ist.

Aufzeichnung der Ergebnisse:

Für die Auswertung können mit JPerf Diagramme Datenrate und Verzögerung über die Zeit erstellt werden. Zudem werden Details zu den einzelnen Segmenten als String ausgegeben und können abgespeichert werden. Der gesamte Testablauf kann mit Capture Solution (siehe Seite 50) aufgezeichnet werden. Dadurch ist eine sekundengenaue Auswertung der Testergebnisse möglich.


MAC-Adressen der Funkmodule
Originator-Abfrage:
Abgefragter AP
MAC-Adresse
(Metrik)
0-255
Erreichbarkeit:
direkt (gleiche MAC) / indirekt (andere MAC)
SSH-Sessions:
Mobiler AP 971 (Oben)
Backbone AP 969 (Mitte)
Backbone AP 968 (Unten)
Ping-Abfrage des Mobilen AP mit Windows CLI
Kontrolle des IP-Traffic an der Netzwerkkarte
Aufzeichnung mit Capture Solution
Bildereinstellungen
Wowza Media Server

7 Hauptteil – Resultate

7.1 Controllerbasiertes WLAN von Aruba

WLAN auf 2.4 GHz

Bei den Tests mit der Controllerbasierten Aruba-Lösung und dem Broadcom WLAN USB-Stick konnten auf 2.4 GHz mit JPerf TCP Datenraten von ca. 16 MBit/s im Stillstand erreicht werden. Bei den Handovertests mit JPerf TCP zeige sich, dass beim Wechsel von einem AP zum nächsten die Datenrate stark einbricht, um dann direkt wieder anzusteigen. Das gleiche Verhalten konnte beim Streaming mit UDP und einer Datenrate von 5 MBit/s beobachtet werden.

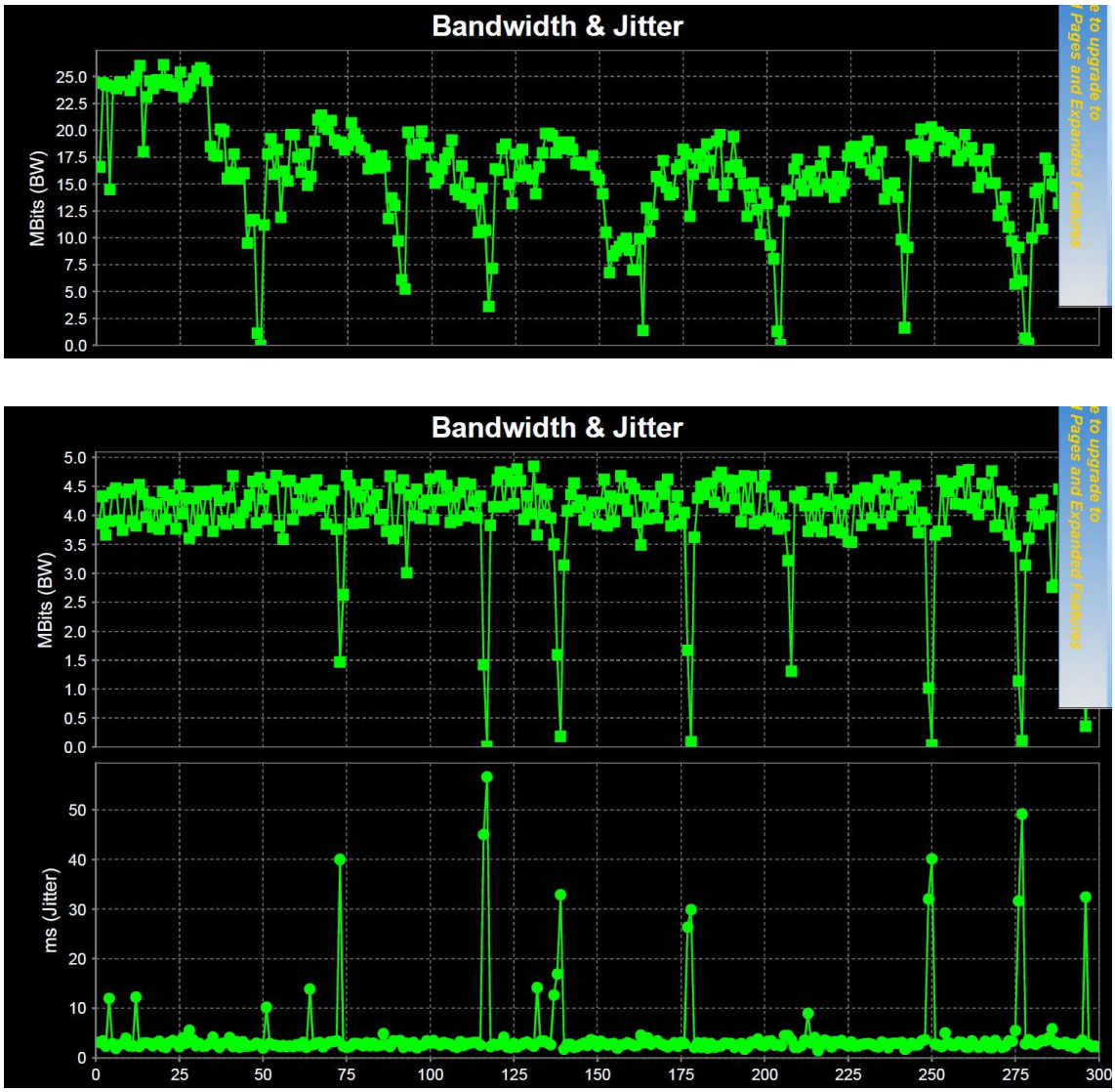


Abbildung 30: Teststreams JPerf TCP/UDP Controllerbasiertes Aruba und USB-Stick

Bei den Tests mit RTMP-Videostreaming von 5 MBit/s und einem Puffer von 1000ms kann die Stabilität des Systems nicht gewährleistet werden: Generell sind beim Handover kurze Einbrüche in der Datenrate zu beobachten, wie auch bei synthetischen Streams mit JPerf. Diese kurzen Einbrüche führen zu Rucklern bei der Ausgabe des Bildes. Diese Ruckler können mit höheren Empfangspufferwerten (3000ms) am Decoder prinzipiell verarbeitet werden.

Bei Durchläufen mit mehrmaligem Wechsel zwischen den Accesspoints ist allerdings zu beobachten, dass es zu größeren Einbrüchen der Datenrate beim Handover kommen kann. Diese größeren Einbrüche verursachen einen Neustart des Streams am Wowza. Vereinzelt waren Neustarts des Encoders zu beobachten.

Im Vergleich dazu brachten Tests mit einem unverschlüsselten Netzwerk keine Vorteile. Beim Testen mit JPerf TCP- und UDP-Streams kam es ebenfalls zu Einbrüchen bei der Datenrate. Auch der Wowza konnte beim Videostreaming nicht stabilisiert werden.

WLAN auf 5 GHz

Auf 5 GHz konnten deutlich höhere Datenraten bis 40MBit/s erzielt werden. Allerdings konnte kein Handover erzielt werden: Bei den Tests mit dem Netgear WNCE 3001 kam es zu großen Abbrüchen bei Test-Streams mit TCP. Dabei fiel auf, dass JPerf erst nach ca. 10 Sekunden Einbruch die Verbindung zwischen Client und Server trennte. Bei Einbrüchen kleiner 10 Sekunden konnte die Verbindung aufrechterhalten werden. Videostreaming auf 5 GHz war daher nicht erfolgreich. Ein Handover konnte zwar vereinzelt erzielt werden, war jedoch nicht reproduzierbar. Ein häufiges Bild war, dass der Handover bei dem ersten AP zum zweiten klappte, aber umgekehrt fehlschlug.

Die großen Einbrüche hatten auch Einfluss auf die CodeOne Software: Bei kurzen Aussetzern kam es zu kurzen Rucklern im Bild, bei Aussetzern bis zu 3 Sekunden startete sich der Wowza neu. Bei Einbrüchen größer 3 Sekunden starteten sich Encoder und Wowza neu, Bei Einbrüchen größer 10 Sekunden kam es zum Verbindungsabbruch: Encoder und Decoder mussten manuell neugestartet werden.

7.2 IAPs

Die Aruba IAPs unterstützen den 11n Standard. Mit dem Broadcom USB-Stick konnten Datenraten von maximal 30MBit/s erzielt werden. Die Übernahme von IP-Adressen vom DHCP Server erfolgt problemlos, genau wie der Aufbau des Meshs.

7.2.1 2+1

WLAN auf 2.4 GHz

Ähnlich wie bei der Aruba Controller-Lösung treten auf 2.4 GHz beim Streaming mit dem Broadcom USB-WLAN-Stick beim Wechsel zwischen den IAPs kurze Einbrüche bei der Datenrate auf. Bei Videostreaming mit RTMP und einem Empfangspuffer von 1000ms kommt es daher zu kurzen Rucklern bei der Bildausgabe am Decoder. Die anderen Software-Komponenten Wowza und Encoder sind davon nicht betroffen. Die kurzen Ruckler können mit einer Erhöhung des Empfangspuffers auf 3000ms prinzipiell verarbeitet werden. Allerdings kann die Stabilität des Systems nicht gewährleistet werden: Bei mehrmaligem Wechsel zwischen den Accesspoints kann es zu größeren Unterbrechungen bei der Datenrate kommen: Diese Aussetzer führen bei RTMP-Streaming zu einem Neustart des Streams am Wowza, was zu einer großen Unterbrechung führt. Diese Neustarts des Wowza treten allerdings seltener auf als bei der Controller-Lösung, das System ist also insgesamt stabiler.

WLAN auf 5 GHz

Auf 5 GHz ähnelt das Verhalten 2.4 GHz: Zwar konnte bei TCP-Messungen mit JPerf kein Handover erzielt werden. Ein Grund dafür könnte sein, dass sowohl die Kommunikation mit dem Klient, als auch die Mesh-Kommunikation auf dem gleichen Kanal stattfand: Maximal konnten Datenraten von 35 MBit/s erzielt werden, das bedeutet, dass der Kanal 44+ zwischenzeitlich mit über 70 MBit/s belastet war. Mit UDP und einer Begrenzung der Datenrate auf 5 MBit/s konnte Handover dagegen stabilisiert werden. Das reibungslose Zusammenspiel der Softwarekomponenten Encoder, Wowza und Decoder bei Videostreaming mit RTMP und einer Datenrate von 5 MBit/s kann allerdings nicht gewährleistet werden: Zwar ist ein Handover prinzipiell möglich und kurze Ruckler können mit einem großen Empfangspuffer ausgeglichen werden. Allerdings kann es bei mehrmaligem Wechsel wie bei 2.4 GHz zu größeren Aussetzern und dadurch zum Neustart des Streams am Decoder kommen.

7.2.2 3APs

Im Webinterface der IAPs kann die Mesh-Verwaltung der APs und damit das Handoververhalten des Aruba-Mesh nicht nachvollzogen werden. Allerdings sollte sich beim Handover des mobilen AP von einem AP zum nächsten die Datenrate halbieren bzw. verdoppeln weil die Anzahl von Hops um eins steigt bzw. abnimmt (siehe Abbildung 12). Die Halbierung bzw. Verdopplung der Bandbreite konnte mit JPerf-TCP-Streams nachvollzogen werden:

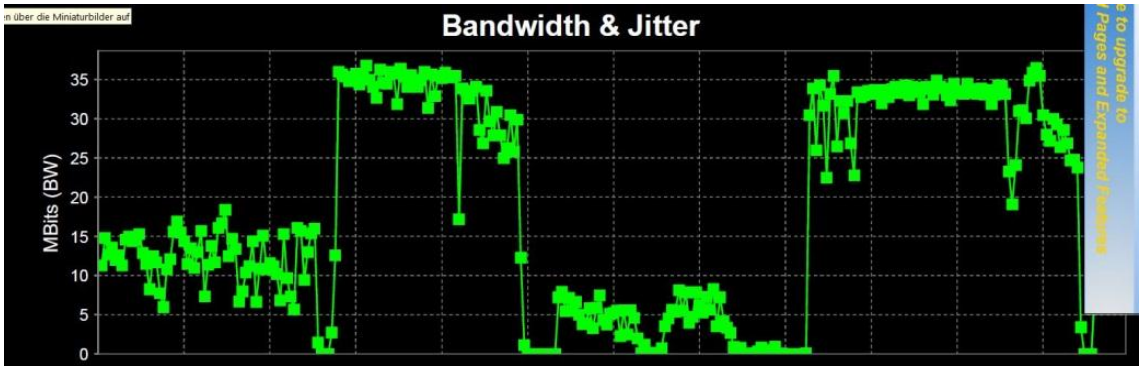


Abbildung 31: JPerf: Handover Aruba IAPs: 3APs mit TCP

Allerdings erfolgt die Umschaltung nur mit großen Einbrüchen in der Datenrate: Die Ummeldung von einem AP zum nächsten benötigt mindestens 3 Sekunden Zeit. Zudem können nach dem zweiten Wechsel keine Datenraten von 15 MBit/s erzielt werden. Auch Tests mit UDP und einer konstanten Datenrate von 5 MBit/s waren nicht erfolgreich:

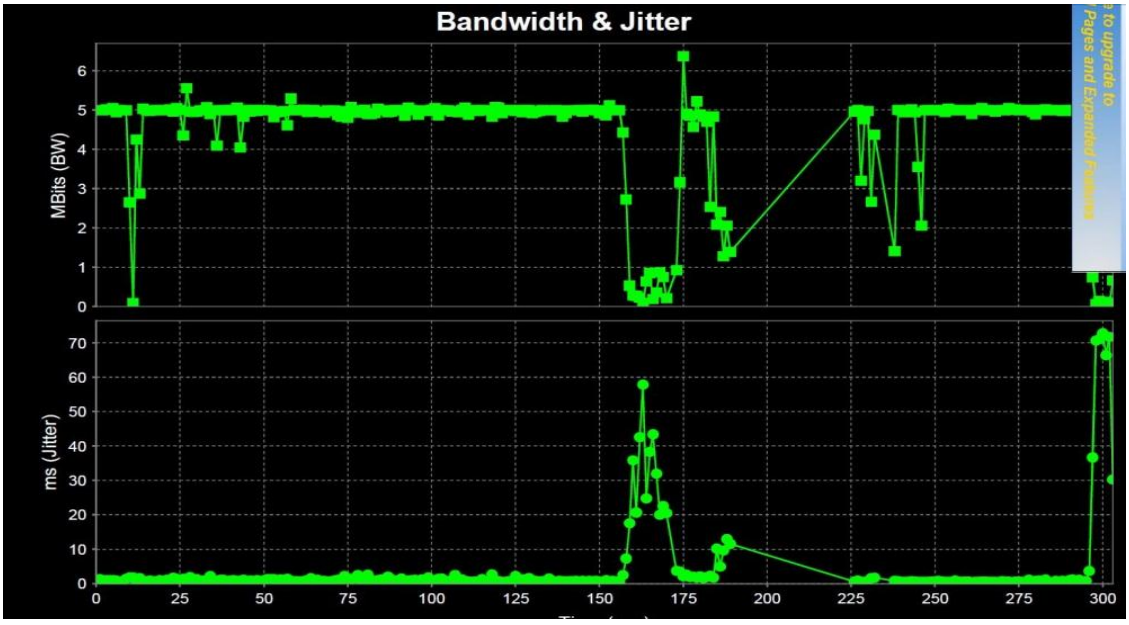


Abbildung 32: JPerf: Handover Aruba IAPs: 3APs mit UDP

Hier kam es zu größeren Einbrüchen bei der Datenrate. Bei späteren Tests können zwar konstante Datenraten erzielt werden. Allerdings ist davon auszugehen, dass vom ARM Anpassungen in der Sendeleistung bei den APs vorgenommen wurden. Durch die Erhöhung der Sendeleistung konnte die ganze Testumgebung von einem AP abgedeckt werden. Dadurch wurde Handover schlichtweg überflüssig.

7.3 Airberry

Generell war bei den Tests mit den Mesh-Routern der Firma Airberry zu beobachten, dass der Datendurchsatz bei 5 GHz höher ist als bei 2.4 GHz. So sind im Backbone (968←→969) bei 5 GHz bis zu 22MBit/s an Datendurchsatz möglich. Dieser Datendurchsatz liegt nah an der theoretisch möglichen Nettodatenrate von 24,4 MBit/s.[61] Bei 2.4 GHz sind maximal 15MBit/s möglich. Bei Erhöhung der Anzahl der Accesspoints und dadurch der Anzahl der Hops, halbierte sich die Datenrate auf Werte von ca. 11MBit/s bei 5 GHz und ca 7,5 MBit/s bei 2.4 GHz (Siehe Abbildung 12). Diese Aussagen stehen im Widerspruch zu den ermittelten Metrik-Werten. Die Metrik-Werte sinken bei 2.4 GHz nicht unter 200, bei 5 GHz konnten Metrikwerte kleiner 150 ermittelt werden. Das heißt: Trotz geringerer Stabilität des Backbones können auf 5 GHz höhere Datenraten erreicht werden als auf 2.4 GHz. Die Datenrate der Test-Streams von 5 MBit/s sollte jedoch von beiden Systemen verarbeitet werden können.

Handover erfordert eine stabile und direkte Backboneverbindung zwischen 968 und 969. Erfahrungswerte für eine stabile Backboneverbindung sind Metrikwerte größer 200.

7.3.1 2+1

WLAN auf 2.4 GHz

Die Handovertests mit dem Broadcom WLAN USB-Stick auf 2.4 GHz und einem Mesh-Backbone auf 5 GHz waren prinzipiell erfolgreich. Anhand der Überwachung der MAC-Adresse des USB-Sticks mit Putty konnte ein reibungsloser Handover des USB-Sticks festgestellt werden. Bei Tests mit JPerf zeigte sich jedoch, dass der Wechsel von einem Accesspoint zum nächsten einen kurzen aber deutlichen Einbruch der Datenrate verursacht: Die Datenrate sinkt für ca. 1 Sekunde von 5MBit/s stark ab und um dann

[61] Vgl. Rech, Seite 409

direkt wieder auf 5 MBit/s anzusteigen. Dieses Verhalten war sowohl mit TCP als auch mit UDP zu beobachten.

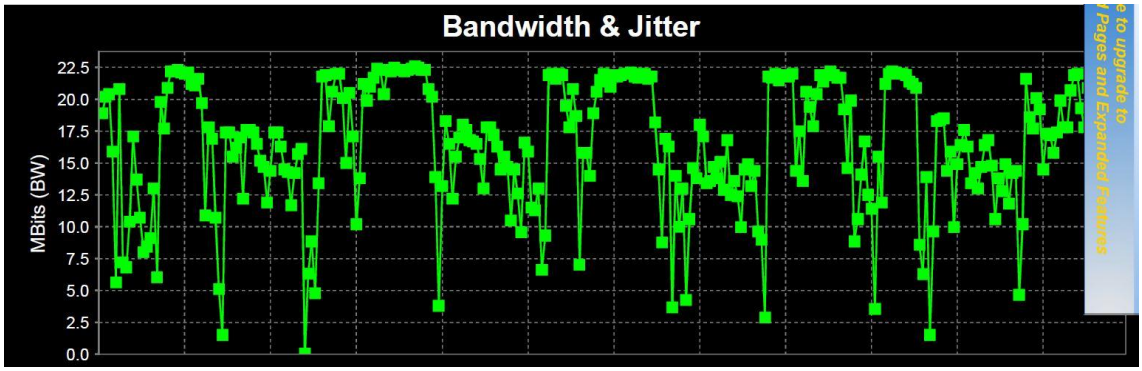


Abbildung 33: USB Stick am BPK 1: TCP

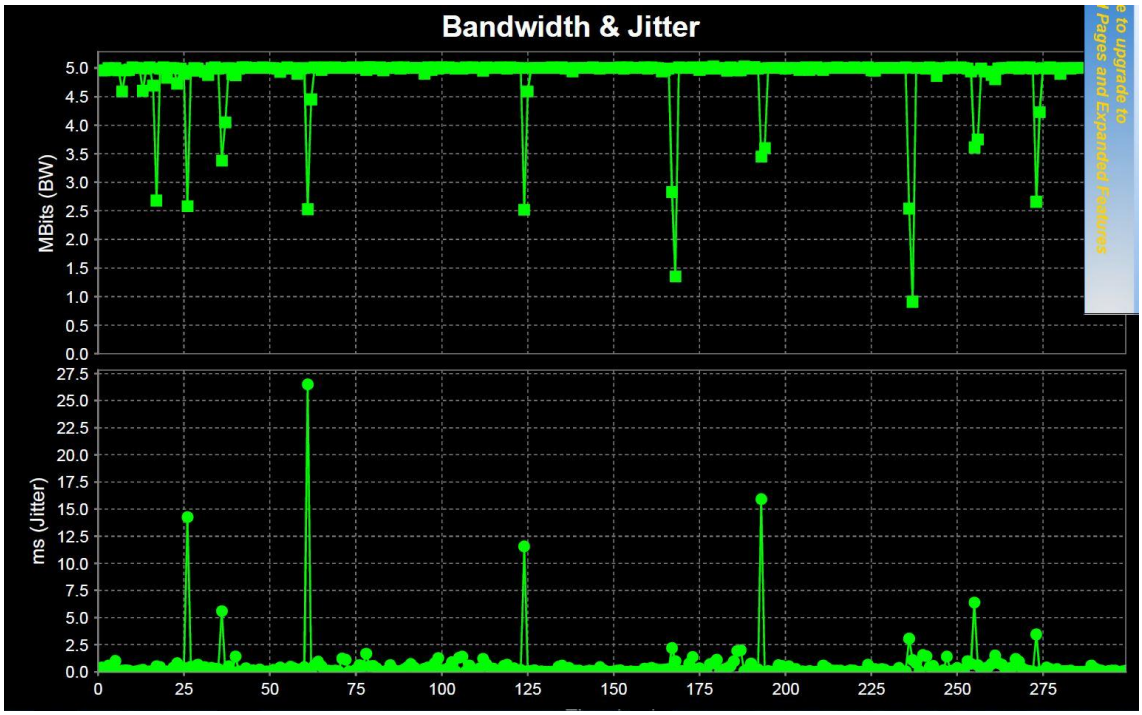


Abbildung 34: USB-Stick am BPK1: UDP 5MBit/s

Bei den Videostreaming-Tests zeigte sich, dass der Einbruch der Datenrate keinen Einfluss auf die Streaming-Sessions hat. Der Encoder funktioniert reibungslos, auch der Wowza läuft stabil. Lediglich bei der Ausgabe des Bildes am Decoder kommt es zu kurzen Rucklern des Videos. Diese kurzen Ruckler können durch die Erhöhung des Puffers am Decoder auf 3000 ms allerdings vermieden werden. Neustarts des Streams am Wowza waren nicht zu beobachten, das System läuft somit stabil.

WLAN auf 5 GHz

Ein Handover bei einem Betrieb des WLAN-Sticks auf 5 GHz und einem Mesh-Backbone auf 2.4 GHz war dagegen nicht erfolgreich: Bei den Putty-Sessions wurden Verzögerungen beim Handover festgestellt. Dadurch kam es bei den Testversuchen mit der CodeOne Technik zu Abbrüchen und Neustarts bei den Streaming-Sessions.

7.3.2 3APs

Handovertests mit einem mobilen Accesspoint als Client stellten sich als besonders schwierig heraus. Tests in der Standardkonfiguration Mesh auf 5 GHz und OGM-Interval von 1000ms waren nicht erfolgreich: Bei der Umschaltung kam es zu großen Störungen: Einerseits gab es große Einbrüchen bei der Datenrate der Test-Streams. Auch die Überwachung der Accesspoints verlief nicht stabil: Während der Umschaltung zwischen den Accesspoints kam es zu regelmäßigen Abstürzen der SSH-Sessions, zudem war der mobile Accesspoint zwischenzeitlich nicht über Ping erreichbar (Zeitüberschreitung der Anforderung). Eine Verkürzung des OGM-Intervalls brachte zwar leichte Fortschritte, ein stabiler Handover konnte jedoch nicht herbeigeführt werden:

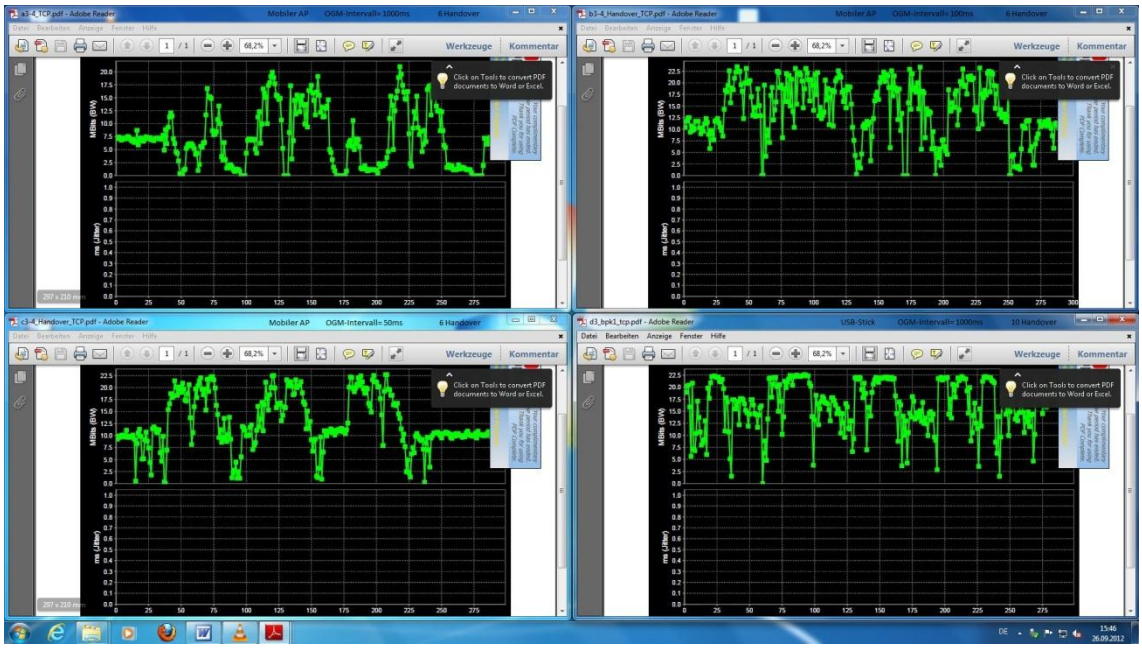


Abbildung 35: OGM-Vergleich TCP

Abbildung 35 zeigt die Auswirkungen der Verkürzung des OGM-Intervalls auf die Datenrate eines TCP-Test-Streams: 1000ms (links oben), 100ms (rechts oben), 50ms (links unten), USB-Teststreaming (rechts unten).

Umschaltung direkte / indirekte Kommunikation:

Die Ursache für die großen Ausfälle ist, dass die Kommunikation des Backbones nicht direkt stattfindet (grün) sondern über den mobilen AP umgeleitet wird (rot), siehe Abbildung 30. Dieses Risiko besteht bei einzelnen Funkverbindungen sowohl auf 2.4 als auch auf 5 GHz. Sobald der mobile AP außer Sichtweite von einem Backbone AP ist, kann eine Verbindung zwischen diesen beiden Routern nicht mehr funktionieren (rot gestrichelt). Auch die Backbone-Verbindung ist davon betroffen. Daher muss das Mesh möglichst schnell auf eine direkte Kommunikation zwischen den Mesh-Routern zurückschalten (grün gestrichelt). Nach bisherigen Erfahrungen besteht das Risiko, dass diese Umschaltung zu spät erfolgt, daraus resultieren der Datenverlust und der Absturz der SSH-Session. Das Risiko für das zu späte Zurückschalten ist bei 5 GHz höher als bei 2.4 GHz, da die Metrik auf 2.4 GHz besser ist.

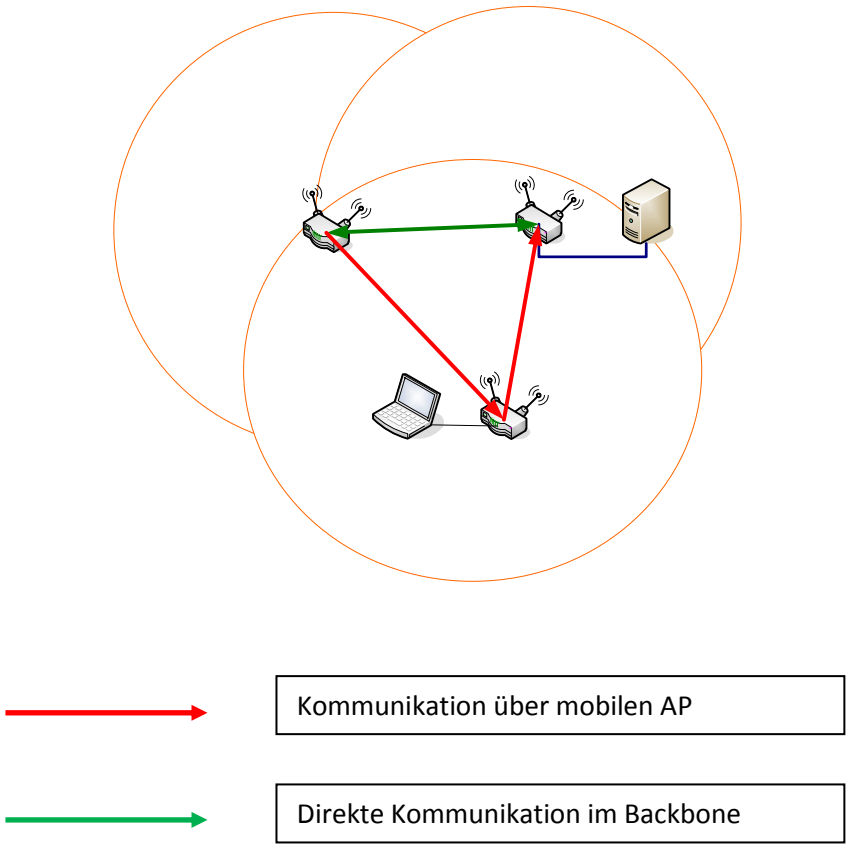


Abbildung 36: Airberry Client mit Sichtverbindung zu beiden Backbone-Routern

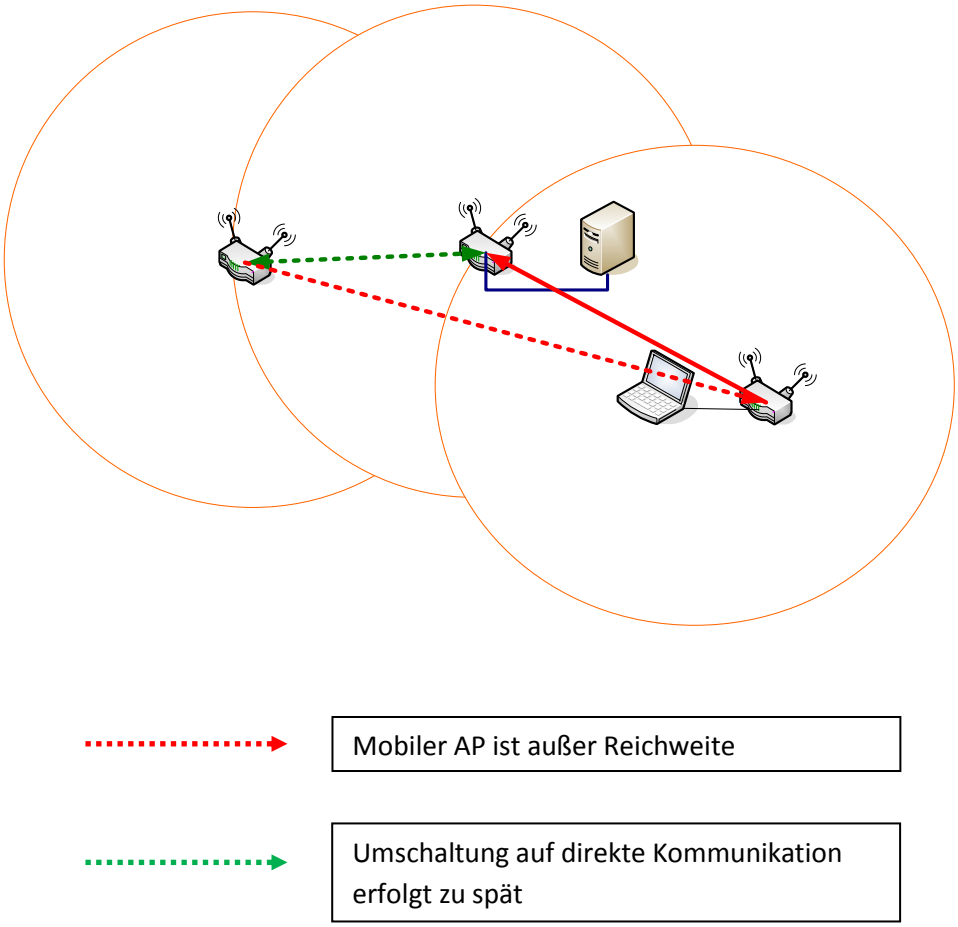


Abbildung 37: Airberry Client mit Sichtverbindung zu einem Backbone-Router

Eine einzelne Funkverbindung kann die Umleitung der Daten über den mobilen AP 971 nicht ausschließen, sowohl auf 5 GHz als auch auf 2.4 GHz. Ein stabiler Handover kann bisher nur über die Kombination Funk und Ethernet-Verkabelung des Backbone gewährleistet werden. Mit dieser Lösung und einem OGM-Interval von 100ms können konstante Datenströme erreicht werden, auch bei einer Pufferlänge von 1000ms.

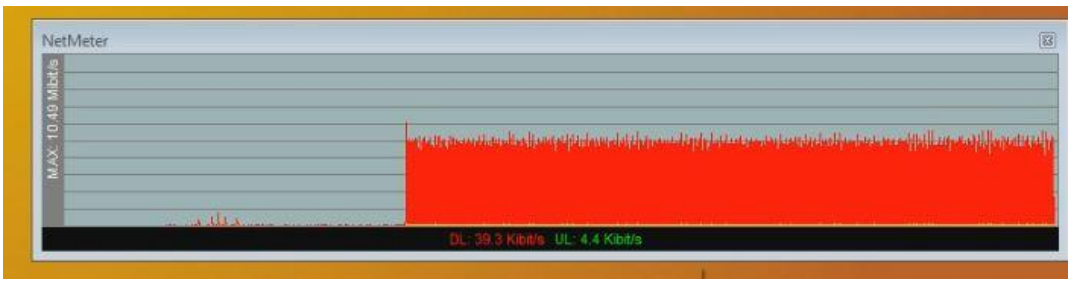


Abbildung 38: Screenshot Netmeter: Datenrate bei Airberry Handover mit Ethernet

8 Fazit

Nun sollen die Resultate zusammengefasst werden, anschließend folgt eine Untersuchung auf Tauglichkeit innerhalb der CodeOne Produktionsbedingungen. Als letztes gibt es einen Ausblick auf die weitere Vorgehensweise.

8.1 Zusammenfassung der Resultate

Für Videostreaming mit WLAN muss ein möglichst unterbrechungsfreier Handover unter Last funktionieren. Dieser Handover konnte sowohl mit einer Lösung aus zwei Accesspoints und einem Client als auch mit einer Mesh-Lösung aus zwei Backbone-Accesspoints und einem mobilen Accesspoint erreicht werden.

Beim direkten Vergleich zwischen „echten Mesh-Lösungen“ und klassischen Infrastruktur-Lösungen spielt die Airberry-Mesh-Lösung ihre wichtigsten Vorteile aus: Alle Mesh-Teilnehmer sind gleichberechtigt, dadurch wird das Management beim Handover extrem vereinfacht: Erstens findet keine erneute Authentifizierung statt, zweitens entscheidet das ganze System und nicht nur der Client, wann der Wechsel zwischen den Accesspoints stattzufinden hat. Drittens funktioniert das ganze System als Gleichwellennetz, ein Frequenzwechsel ist nicht erforderlich. Ein unterbrechungsfreier Handover mit zwei Backbone-Accesspoints und einem mobilen Accesspoint kann dadurch sowohl auf 2.4 GHz als auch auf 5 GHz erzielt werden. Voraussetzung hierfür ist, dass die Backbone-Router über Ethernet miteinander verbunden werden. Dieser Workaround schafft Redundanz, zudem sind konstant hohe Datenraten möglich, da keine Hops stattfinden müssen.

Systemlösungen für Handover aus zwei Accesspoints und einem Client sind ebenfalls prinzipiell funktionsfähig. Wie in Kapitel 4.7 beschrieben, spielt bei den untersuchten Clients jedoch die fehlende Unterstützung von 802.11i Roaming-Mechanismen eine große Rolle: Beim Wechsel eines Clients von einem Accesspoint zum nächsten wird nicht nur die Frequenz an den neuen AP angepasst, sondern auch der Pairwise Master Key neu generiert. Dieser Prozess benötigt mindestens 700ms Zeit. In diesem Zeitraum bricht die Datenrate stark ein und es kommt zu kurzen Rucklern bei der Videoübertragung. Eine Lösung für dieses Problem ist die Anhebung des Empfangspuffers am Decoder von 1000ms auf 3000ms, dadurch können Bildruckler vermieden werden.

Hauptaugenmerk besteht weiterhin darin, die Zuverlässigkeit eines Systems, dass aus Accesspoints, Client, und CodeOne Software besteht zu optimieren: Bisher kann diese Zuverlässigkeit durch die Kombination Netgear WNDA 3100 USB-Stick mit Broadcom BCM4323 Chipsatz und Airberry Mesh-Routern im Zusammenspiel mit Wowza Media

Server und Code One Decoder gewährleistet werden. Auch bei der Unterstützung der verschiedenen Frequenzbereiche zeigen sich Unterschiede: Für einen zuverlässigen Handover sollte bei der genannten Kombination der Frequenzbereich 2.4 GHz gewählt werden. Daher sollte unbedingt nach weiteren Dual-Band Clients, vorzugsweise mit Unterstützung von 802.11i Authentifizierung, recherchiert werden.

8.2 WLAN innerhalb der CodeOne Produktionsbedingungen

Damit WLAN auf einer Produktion Anwendung finden kann, ist Betriebssicherheit ein grundlegender Faktor. Diese Betriebssicherheit setzt sich zusammen aus einem sicheren Handover sowie möglichst wenig Störungen durch fremde WLAN-Netze. Die Betriebssicherheit kann mit der Airberry-Mesh-Lösung mit zwei Backbone-Accesspoints und einem mobilen Accesspoint gewährleistet werden: Die Übertragung von konstanten Datenströmen ist möglich, da beim Handover keine Authentifizierung stattfindet. Dadurch kann die Zuverlässigkeit des Wowza Media Servers gewährleistet werden. Zum anderen funktioniert diese Lösung auch auf 5 GHz. Videostreaming setzt hohe Datenraten und sichere Echtzeitübertragung voraus. Der 5 GHz-Frequenzbereich bietet höhere Bandbreiten und weniger Störungen durch Consumer-WLAN als das ISM-Band und ist daher für die professionelle WLAN-Nutzung dringend zu empfehlen.

Ein weiterer Faktor, der bei Produktionen wichtig ist, ist die Latenzzeit. Generell gilt: Bei Live-Übertragung kann eine hohe Latenzzeit nur dann vernachlässigt werden, wenn der Zuschauer keinen direkten Vergleich zum Ort des Geschehens hat, beispielsweise bei Webcast-Anwendungen mit einer Kamera. Auch hier ist der fehlende Authentifizierungsvorgang bei Airberry besonders vorteilhaft. Bei konstanten Datenströmen sind weniger Paketverluste zu erwarten, daher kann der Empfangspuffer sehr klein gehalten werden und bringt bei 1000ms zufriedenstellende Ergebnisse.

Bei Mehrkameraproduktionen muss das Signal einer drahtlosen Kamera möglichst mit drahtgebundenen Kameras gemischt werden können. Daher kann eine generelle Aussage, ob sich eine WLAN-Systemlösung für Mehrkameraproduktionen eignet, bisher nicht getroffen werden: Im Vergleich zu DVB-T-Drahtloskameras ist die Latenzzeit von WLAN um Faktor zehn höher. Deshalb hängt es vom konkreten Anwendungsfall ab, ob WLAN eingesetzt werden kann. Denkbar wäre zum Beispiel der Einsatz von WLAN zur Übertragung einer Live-Schalte von einer Karnevalsparty aus einer der zahlreichen Kneipen der Düsseldorfer Altstadt.

Der bisherige Workaround mit der Airberry-Mesh-Lösung sieht die Ethernet-Verkabelung der Backbone-Router zusätzlich zur Funkverbindung vor. Dadurch ist

sehr viel Planungsaufwand notwendig, allerdings kann so Redundanz erreicht werden. Zudem finden keine Hops mehr statt (siehe Abbildung 12). Daher kann an allen Backbone-Routern die gleiche hohe Datenrate erzielt werden. Bisher konnten bei Airberry ein Handover nur mit Datenraten von 5 MBit/s erzielt werden, dadurch ist ein Betrieb von mehreren Videostreaming-Einheiten gleichzeitig und mit ausreichender Qualität nicht möglich. Bei der Teststellung handelte es sich um 11a,g Funkmodule mit einer Nettodatenrate von rund 25 MBit/s. Es ist davon auszugehen, dass der parallele Betrieb von mehreren Videostreaming-Einheiten mit 11n Funkmodulen und einer Nettodatenrate von über 300 MBit/s problemlos möglich sein wird.

Zum Schluss der Untersuchungen im Dezember ist damit begonnen worden, einen weiteren WLAN-Chipsatz, Intel Centrino Ultimate-N 6300, auf Handoververhalten zu untersuchen. Dieser Chipsatz unterstützt ebenfalls keine 802.11i Roaming-Mechanismen, es kommt also zu kurzen Einbrüchen der Datenrate bei dem Wechsel zwischen zwei Accesspoints. Der Intel-Chipsatz wurde bisher nur mit den Aruba-Lösungen getestet, da er bei der Teststellung von Airberry noch nicht zur Verfügung stand. Bei ersten Tests mit den Aruba IAPs konnte ein zuverlässiger Handover auch auf 5 GHz erreicht werden: Der Wowza Media Server lief stabil, doch auch hier kam es zu kurzen Rucklern bei der Bildausgabe.

8.3 Ausblick

Die Mesh-Router der Firma Airberry werden nach Herstellerangaben mit einer neuen Firmware ausgestattet werden. Um Aussagen über die Tauglichkeit der Airberry-Mesh-Lösung innerhalb der CodeOne Produktionsbedingungen zu erhalten, muss also zwingend ein abschließender Test mit der neuen Firmware-Version erfolgen. Als nächstes muss Videostreaming mit höheren Datenraten als 5 MBit/s untersucht werden und ein paralleler Betrieb von mehreren Videostreaming-Einheiten muss getestet werden. Dafür sind 11n-Funkmodule notwendig. Ein dritter, sehr interessanter Punkt wird die Beantwortung der Frage sein, ob die bisher nötige Ethernet-Verkabelung der Backbone-Router durch eine weitere 5GHz-Funkstrecke ersetzt werden kann. Dafür sind zwei Dual-Band-WLAN-schnitten an den Routern erforderlich. Als letzter Punkt sollte untersucht werden, ob der Backbone durch beliebig viele Router erweitert werden kann.

Zweitens sollte der Intel Centrino Ultimate-N 6300 in weiteren 2+1 Testszenarios untersucht werden. Hierbei sollten vor allem Performance-Unterschiede auf 5 GHz zwischen Airberry und Aruba betrachtet werden, da die Airberry-Lösung mit der alten Firmware und 11a Funkmodulen hier bisher die größten Schwächen gegenüber Aruba gezeigt hat. Sofern eine stabile 2+1 Lösung auf 5 GHz gefunden wurde, kann außerdem damit begonnen werden genauere Einstellungen am Empfangspuffer vorzuneh-

men, mit dem Ziel einen Schwellwert für einen Empfangspuffer kleiner 3000ms zu finden, bei dem eine flüssige Bildausgabe am Decoder erfolgt.

Sämtliche Tests fanden innerhalb der CodeOne Räumlichkeiten mit kleinen Sendeleistungen statt. Mit der Airberry Mesh-Lösung wurde ein System gefunden, dass sich bei größeren Produktionen, größeren Gleichwellen-Netzen und mehr Sendeleistung beweisen kann. Erst durch den Einsatz von einer WLAN-Systemlösung in der Produktion kann überprüft werden, inwieweit sie sich als Ergänzung oder sogar als Konkurrenz zu bestehenden Systemlösungen eignet.

Literaturverzeichnis

Airberry_mesh: Whitepaper Einführung in Mesh Netzwerke: URL: http://airberry.com/downloads/airberry_Whitepaper_DE_02_Wireless_Mesh.pdf, abgerufen am 21.12.2012.

Aruba Networks: ArubaOS 6.1 User Guide, 2011.

Aruba Networks: Interoperabilität URL: http://arubanetworks.com/support-services/interoperability, abgerufen am 16.08.2012.

Aruba Networks: Aruba 650 Controller Data-Sheet URL: http://www.arubanetworks.com/pdf/products/DS_A650651.pdf, abgerufen am 26.10.2012.

Blaeß, Ivo: Serversysteme und Vernetzungskonzepte für die Produktion mit Videomaterial in SD- und HD-Qualität der Fakultät Medien der Hochschule Mittweida, Bachelorarbeit, Hochschule Mittweida, 2009.

Bönninghoff, Arne: Ortsunabhängige Live-Videoübertragung, Diplomarbeit, FH Düsseldorf, 2011.

Bundesbreitbandbüro: Breitband via Satellit. URL: www.breitbandbuero.de, abgerufen am 03.08.2012.

Bundesnetzagentur: WLAN: URL: http://www.bundesnetzagentur.de/DE/Presse/Publikationen/service/WLANFunkanwendungen/WLANFunkanwendungen_node.html, abgerufen am 02.01.2013.

Cisco: CCNA Exploration 4.0 Network Fundamentals, Chapter 1.3.3: Converged Networks, Cisco Systems, 2009.

HSMWiki:URL: https://wiki.hs-mittweida.de/index.php/Eduroam-Einrichtung_unter_Windows_7, abgerufen am 30.07.2012.

Inmarsat: BGAN Global Voice and Broadband Data, 2009 URL: http://www.inmarsat.com/services/BGAN, abgerufen am 14.12.2012.

Kafka, Gerhard: WLAN, Hanser, 2005.

Leykam, Christian: IP-basierte Live-Videoübertragung in lokal installierten, drahtlosen Netzwerken, Diplomarbeit, FH Düsseldorf, 2012.

Linksys.info: Broadcom Wireless LAN Adapter User Guide, URL: http://www.linksysinfo.org/index.php?threads/broadcom-wireless-lan-adapter-user-guide.15819/, Eintrag vom 11.06.2005, abgerufen am 05.11.2012.

Lüders, Christian: Lokale Funknetze, 1. Auflage, Vogel, 2007.

Meixelsberger, René: Einsatzmöglichkeiten einer DVB-T basierten Funkstrecke an der Hochschule Mittweida, Bachelorarbeit, Hochschule Mittweida, 2008.

Open Mesh: URL: http://www.open-mesh.org/projects/batman-adv/wiki/Wiki, abgerufen am 24.10.2012.

Perkins, Colin: RTP Audio and Video for the Internet, Pearson Education, 2008.

Rech, Jörg: Wireless LANs, 3. Auflage, Heise, 2008.

Sauter, Martin: Grundkurs Mobile Kommunikationssysteme, 4. Auflage, Viewig+Teubner, 2011.

Stüntz, Hermann: Analyse der Fast BSS Transition in WLAN Infrastrukturen, Forschungsprojekt, FH Köln, 2011, URL: http://www.dn.fh-koeln.de/download/arbeiten/Hermann_Stuenz_2011.pdf, abgerufen am 13.12.2012.

Tooway: toowaysat.com, abgerufen am 07.12.2012.

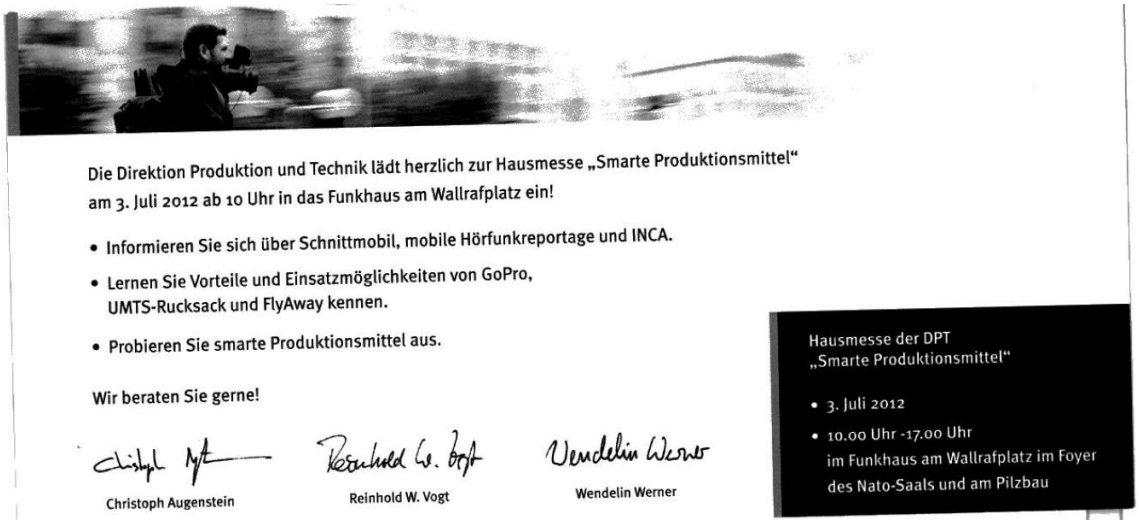
WDR Flyer: Hausmesse der DPT, „Smarte Produktionsmittel“ am 03.08.2012 (siehe Anhang).

WDR Print: „Die Smarte Fernsehtechnik des WDR“, URL: http://www1.wdr.de/unternehmen/service/publikumsservice/infomaterial/wdrprint122.pdf, abgerufen am 10.12.2012.

Wikipedia: Geostationärer Orbit, URL: de.wikipedia.org/wiki/Geostationärer_Satellit, abgerufen am 03.08.2012.

Winkler, Lutz: WLAN, Lehrunterlagen der Fakultät EIT der Hochschule Mittweida.

Anhang



Die Direktion Produktion und Technik lädt herzlich zur Hausmesse „Smarte Produktionsmittel“ am 3. Juli 2012 ab 10 Uhr in das Funkhaus am Wallrafplatz ein!

- Informieren Sie sich über Schnittmobil, mobile Hörfunkreportage und INCA.
- Lernen Sie Vorteile und Einsatzmöglichkeiten von GoPro, UMTS-Rucksack und FlyAway kennen.
- Probieren Sie smarte Produktionsmittel aus.

Wir beraten Sie gerne!

Christoph Augenstein | Reinhold W. Vogt | Wendelin Werner

Hausmesse der DPT
„Smarte Produktionsmittel“

- 3. Juli 2012
- 10.00 Uhr -17.00 Uhr
  im Funkhaus am Wallrafplatz im Foyer des Nato-Saals und am Pilzbau

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe. Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Ort, Datum Vorname Nachname